AN ENTERPRISE ENGINEERING APPROACH TO SAFETY MANAGEMENT

AN ENTERPRISE ENGINEERING APPROACH TO SAFETY MANAGEMENT

BY

PAUL JOANNOU, BASC, M.ENG, P.ENG.

A THESIS

SUBMITTED TO THE DEPARTMENT OF COMPUTING AND SOFTWARE

AND THE SCHOOL OF GRADUATE STUDIES

OF MCMASTER UNIVERSITY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY OF SOFTWARE ENGINEERING

Doctor of Philosophy of Software Engineering (2017) McMaster University

(Computing and Software) Hamilton, Ontario, Canada

TITLE:	An Enterprise Engineering Approach to Safety Management
AUTHOR:	Paul Joannou
	BASc, M.Eng, P.Eng
	McMaster University, Hamilton, Canada
SUPERVISOR:	Dr. Tom Maibaum
NUMBER OF PAGES:	xi, 498

ABSTRACT

Significant accidents are often related to the performance of a complex socio-technical system (enterprise) involving technology, people, organizations, processes, management and legislation.

Approaches to identify factors that lead to accidents and then take them into account during the design, operation, maintenance and evolution of the socio-technical system (enterprise) are not well defined and not consistently utilized in practice.

The emerging discipline of "enterprise engineering" provides an opportunity to apply an engineering approach to the design, operation, maintenance and evolution of enterprises to improve the likelihood of the enterprise achieving and maintaining its safety goals.

The integration of design principles and approaches from the fields of systems engineering, safety engineering, management science and enterprise architecture into a Safety Enterprise Engineering (SEE) approach based on a consistent model of the enterprise provides the basis of the approach described in this thesis.

A general process model for applying an enterprise engineering approach to safety management is defined. Design principles from nuclear industry best practice documents are identified and mapped to the general process model.

The Fukushima nuclear accident that occurred in 2011 was used to identify weaknesses in current practices in the nuclear industry. These weaknesses were compared with best practices, as defined by International Atomic Energy Agency (IAEA) documents, to identify the subset of weaknesses identified from the Fukushima accident that are also weaknesses within the IAEA set of best practices. The Safety Enterprise Engineering approach was applied to a slice of safety related functionality of a CANDU nuclear utility to demonstrate the degree to which the SEE approach overcomes weaknesses of both current practice and best practice within the nuclear industry.

ACKNOWLEDGEMENTS

Working on my PhD has been an enjoyable journey. The journey itself, rather than the destination, was my motivation for undertaking the PhD. It has been a great opportunity for continued learning and growth, a chance to combine my 30 years of engineering experience with the work of others, and a personal challenge to see if I was still up to the challenges of a post graduate program. I would sincerely like to thank all the people that made the journey feasible and enjoyable.

First, I would like to thank my thesis supervisor, Dr. Thomas Maibaum, for guiding me on my PhD journey. Tom, you have been exceptionally supportive during this journey and I truly appreciate your help and all the learning opportunities that you provided me.

I would also like to thank the faculty at the Department of Computing and Software at McMaster for helping me through the required four graduate courses and comprehensive exams. Dr. Jeff Zucker's patience and good humour helped me with Logic & Discrete Math. Coaching from Dr. Bill Farmer and Dr. Ridha Khedri helped me past several barriers to progress.

Another aspect that made the journey enjoyable was working with the excellent staff of the McMaster Centre for Software Certification. I appreciated both the professionalism of Magda, Deepa, and Lynda in the performance of their jobs along with their good nature and friendship. Working with the three principals of the Centre, Dr. Alan Wassyng, Dr. Mark Lawford and Dr. Tom Maibaum, was also a treat. Discussions on what is required to provide grounds for justified confidence that a claim has been or will be achieved for a software intensive system were always interesting. The perspectives provided by each of the three amigos helped provide a more complete perspective to each issue and helped shape my approach within the thesis. I really appreciated the opportunity to facilitate many Software Certification Consortium workshops where perspectives from many of the experts in the area of certification of software intensive systems were presented and discussed.

Finally, I would like to thank my wife Debbie along with my daughters Ashley, Christine and Heather. I would not have made it through the journey without their support, assistance and encouragement.

Contents

List of Figures

List of Tables

1 OVERVIEW

Significant accidents are often the result of the performance of a complex socio-technical system (enterprise) involving technology, people, organizations, business processes, governance and legislation. In the nuclear power industry, it has been observed that:

> "Four decades of analysis and operating experience have demonstrated that nuclear plant core-damage risks are dominated by beyond-design-basis accidents. Such accidents can arise, for example, from multiple human and equipment failures, violations of operational protocols, and extreme external events." [1]

This observation highlights the fact that major accidents are occurring due to complex scenarios of events that were either overlooked or considered of too low a probability to take into account.

The observation also aligns with Leveson's observation about safety engineering in [2] that "While the traditional approaches worked well for the simpler systems of the past for which they were devised, significant changes have occurred in the types of systems". Leveson is highlighting that complex systems have many failures, many combinations of failures and emergent behaviour due to unintended interactions that make traditional safety engineering approaches ineffective.

Achieving safety, relative to a technological system, requires the thorough application of risk management practices in the design, operation, maintenance and modification of the system during its lifetime. Risk management requires that hazards resulting from operation of the system be identified, and then either be eliminated, controlled or mitigated in order to achieve acceptable risk.

Methodical approaches to identify factors that lead to accidents and then take them into account during the design, operation, maintenance and evolution of the socio-technical system (enterprise) are not well defined and not consistently utilized in practice.

The Safety Enterprise Engineering (SEE) approach developed and demonstrated in this thesis incorporates all these factors and focuses on achieving safety over

the entire life of a hazardous system. It is able to deal with the complexity of a socio-technical system and deal with very low probability accidents.

The resulting Safety Enterprise Engineering approach:

- spans the whole lifecycle of a system, and includes both technical and socio-technical factors,
- defines a process for the engineering of an enterprise that is applicable at different levels of abstraction and integrates risk management processes to achieve the enterprise's safety goals,
- incorporates hazard analysis techniques that are applicable to socio-technical systems,
- defines design principles that can be used to eliminate, control or mitigate hazards associated with the enterprise's business processes, organization, governance and technology for which it is responsible,
- provides a definition of a model of an enterprise that focuses on achieving safety and is applicable at different levels of abstraction, and
- defines principles to apply in the design, operation, maintenance and evolution of an enterprise to achieve and maintain its safety goals.

The thesis's hypothesis is that safety goals can be more effectively achieved by applying an engineering approach[1] to the design, operation, maintenance and evolution of the enterprise that integrates applicable principles and practices from safety engineering, systems engineering, management science and enterprise architecture.

The hypothesis is tested by applying the SEE approach to a slice of safety related functionality of a typical nuclear power utility and then assessing the degree to which the approach addresses weaknesses in nuclear industry current and best practices. The accident in 2011 at the Fukushima Daiichi nuclear power plant in Japan is used to identify weaknesses in nuclear industry current practices. These weaknesses are compared to nuclear industry best practice documents to identify weaknesses in nuclear industry best practices.

[1] Professional Engineer Ontario defines the practice of professional engineering as any act of designing, composing, evaluating, advising, reporting, directing or supervising, or the managing of any of these acts wherein the safeguarding of life, health, property, economic interests, the public welfare or the environment is concerned, and that requires the application of engineering principles.

The SEE approach is shown to improve on current and best practice in the nuclear power industry. It is shown to more comprehensively take into account combinations of events and low probability events. It also takes into account interactions between potentially hazardous technologies and the business processes, organizations and governance associated with the technology's design, construction, operations, maintenance and evolution.

Figure 1 shows the structure of the thesis.

Chapters 1 through 4 provide an introduction by presenting this overview, a literature review of disciplines supporting the SEE approach and the lack of alternative approaches that are successful at addressing the safety of socio-technical systems, a description of the research methodology used to define and then demonstrate the SEE approach, and the definition of some terms that are foundational to a common understanding of safety. Appendix 1 shows the key concepts reflected in the source documents from which the definition of terms are based.

Chapters 5 through 7 define the SEE approach by defining the overall SEE process, an approach to hazard analysis that is applicable to socio-technical systems, and the modeling constructs that are used to define the enterprise at different levels of abstraction. Appendix 2 defines for each modelling construct its purpose, key attributes and relationships to other constructs. The SEE approach leverages international standards for systems engineering, risk management and enterprise modeling but integrates them into a coherent approach for safety enterprise engineering. Leveson's STPA hazard analysis [2] approach is integrated into the SEE approach since it is applicable to socio-technical systems.

Chapters 8 through 10 identify nuclear industry best practice principles, and weaknesses in both current practices and best practices in the nuclear industry. Best practices are based on IAEA best practice documents. From the best practice requirements in the IAEA documents, design principles that can be applied within the SEE approach are reverse engineered. Appendix 3 lists requirements from the IAEA documents and the results of reverse engineering the requirements into design principles that can be applied within the SEE approach. The design principles are organized into lifecycle phases, and by whether they primarily impact business process, organizations, governance or technology to aid in their application within the SEE approach. Appendix 4 identifies weaknesses in current nuclear practices by identifying the recommendations for improvement that resulted from the many industry reports that analyzed the Fukushima accident

in 2011. For each weakness, principles from Appendix 3 are identified that would have addressed the recommendation. Weaknesses for which corresponding principles were not found indicate areas where IAEA best practices are weak. Appendix 5 assesses the changes that were made to IAEA documents as a result of Fukushima to help assess the degree to which the changes addressed the identified weaknesses in Appendix 5.

Chapters 11 and 12 present an example of the application of the SEE approach to a typical nuclear power utility and an assessment of the degree to which the example demonstrates the SEE approach's ability to address weaknesses in nuclear industry practices. Appendix 6 describes the design features identified to address the potential causes of unsafe control actions from the example.

Chapter 13 provides overall conclusions, identifies limitations of the conclusions and identifies possible future work.

Note that when figures are used from cited documents, the citation is shown in the caption of the figure.

The SEE approach provides a holistic approach that spans the whole lifecycle of a system and addresses both technical and socio-technical factors that can lead to accidents. The thesis provides a definition of the SEE process to be followed, the models produced by the process and principles that should be incorporated to achieve an enterprise's safety goals.

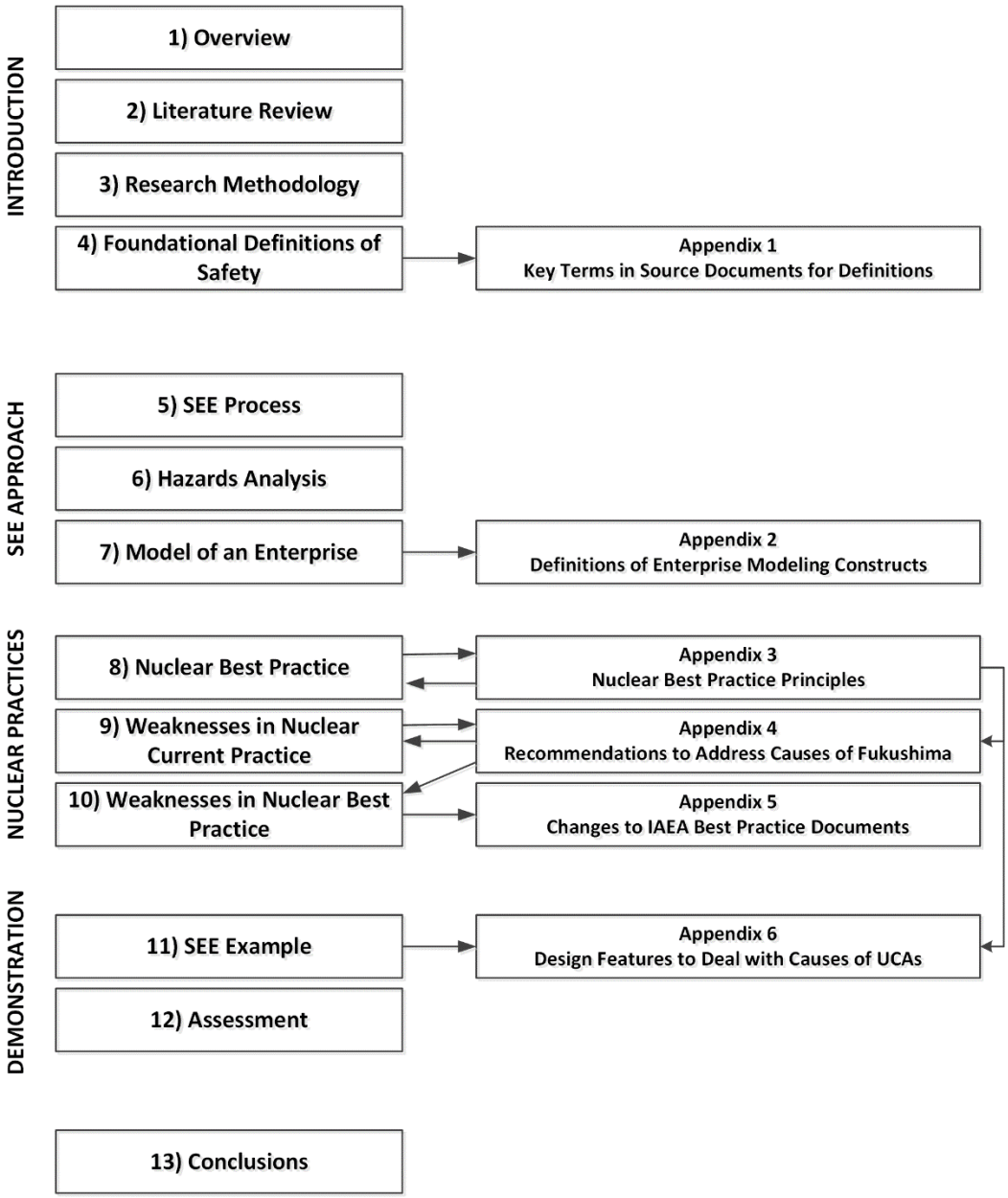


Figure 1 - Structure of Thesis

2 LITERATURE REVIEW

Introduction

The discipline of enterprise engineering is an emerging discipline. It builds upon and integrates work done in the disciplines of systems engineering, safety engineering, management science, enterprise architecture and others [3]. This literature review summarizes the key concepts and principles from these supporting disciplines that are relevant to enterprise engineering focused on achieving safety goals.

Need to Deal with Complex Socio-technical Systems

Traditional safety engineering has focused on identifying failures that can lead to accidents and then strives to reduce the probability of the failures leading to the accident through reliability engineering techniques such as the use of redundancy or mitigating systems [2].

In recent years the increasing complexity of technological systems and changing tolerance for accidents has required different approaches to safety engineering.

> "Accident causation must be viewed as a complex process involving the entire socio-technical system including legislation, government agencies, industry associations, insurance companies, company management, technical engineering personnel, operations, etc" [2].

> "Instead of safety management in terms of preventing component failure events, it is defined as a continuous control task to impose constraints necessary to limit system behaviour to safe changes and adaptations" [2].

The US Nuclear Regulatory Commission also identified the challenges in review of complex systems. "Many of these challenges come from hazards that are rooted in systemic causes, such as inadequacies in engineering organizations, processes and methods." [4] To help improve the review of these complex systems a list of systemic causes of hazards were identified along with conditions that reduce the hazard space. This is very similar to the list of causes of unsafe control actions defined in section 6.3 and the design features to address hazards defined in Appendix 3.

There are some academic initiatives that contribute to achieving safety in an enterprise context such as the DIRC project in the UK (www.dirc.org.uk). DIRC focuses on achieving dependability of complex, computer-based systems taking into account interactions with people. The DIRC project focuses on a set of related topics such as:

- The functioning of socio-technical systems,
- System development processes,
- Extending ethnography,
- Timing in socio-technical systems,
- Dependability assessment and decision making,
- Security and privacy,
- Dependable assistive technology, and
- Dependable service-centric grid computing.

What the project does not do is integrate these topics into a coherent, integrated approach for safety enterprise engineering.

Enterprise Engineering

The emerging discipline of Enterprise Engineering takes into account the complexities associated with engaging organizations of people executing processes supported by technologies to accomplish the goals and objectives of the organization [3].

"Because of its holistic, systematic approach, enterprise engineering resembles systems engineering. But it differs from it in an important aspect; enterprise engineering aims to do for enterprises (which are basically conceived as social systems) what systems engineering aims to do for technical systems." [3]

A key observation is that enterprises are complex adaptive systems for which it is impossible to determine the ultimate (operational) reality of the enterprise down to minute details. Instead one must find appropriate approaches to master enterprise complexity at effective levels.

Since enterprises are created by people, enterprise creation requires design activities. Unfortunately, the importance of design is not generally recognized by management when dealing with enterprises. For an enterprise to achieve its goals

by virtue of a good enterprise design requires some guiding authority (enterprise governance) to mandate the prerequisite design activities [3].

Often enterprises fail to achieve their strategic goals, including safety goals, because of a lack of coherence and consistency among the various components of the enterprise, which precludes it operating as a purposeful, unified and integral whole [5], [6].

There are some key differences that need to be taken into account when designing and operating an enterprise. The complexity of an enterprise results in aggregated behaviour that cannot be inferred from knowledge about the constituent parts. Since enterprises are social systems, communications play an essential role. Cause and effect relationships between elements of an enterprise are numerous, complex, dynamic and have a large degree of uncertainty [7].

"Detailed task and job descriptions are unproductive when predictability vanishes. The capacity for self-organizing is essential for enterprise adaption and change. Employee involvement is essential." [7] This is especially important in establishing a safety culture where decisions of individuals must reflect that safety is an overriding priority.

Enterprise engineering concerns the analysis, optimization, and re-engineering of all parts of the business processes, information systems, and organizational structures in an enterprise. It offers the benefit of achieving a unified and integrated design with clear responsibilities.

The discipline of Enterprise Architecture provides frameworks whose aim is to structure the concepts, activities and tasks required to design and build an enterprise. Some common design views used in enterprise architecture are business, resources, organization, information, data, application and technology views [8], [9].

System and Safety Engineering Disciplines

The system engineering and safety engineering disciplines have achieved a level of maturity relative to their application to technological systems. The challenge of safely engineering complex, socio-technical systems has been recognized over the last decade and approaches to dealing with the challenges are starting to emerge.

Systems engineering provides a definition of a system as “a collection of elements and a collection of inter-relationships amongst the elements such that they can be viewed as a bounded whole relative to the elements around them”. The term “element” is used in its very broadest sense to include anything from simple physical things to complex organisms including people, environments and technologies. An engineered system is recognized as an open system of technical and sociotechnical elements that exhibits emergent properties[2] not exhibited by its individual elements [10], [11].

> “Safety … is clearly an emergent property of systems: Safety can only be determined in the context of the whole. Determining whether a plant is acceptably safe is not possible, for example, by examining a single valve in the plant. In fact, statements about the "safety of the valve" without information about the context in which that valve is used, are meaningless. Safety is determined by the relationship between the valve and the other plant components.” [2]

These systems engineering definitions set the stage for treating an enterprise as a system and to apply systems engineering approaches to its design and evolution. Safety engineering combines system engineering practices with risk management practices to achieve system safety. The traditional practices of systems engineering, safety engineering and risk management are applicable to enterprises, but additional approaches need to be applied to take into account the complexities introduced by including human elements in the system, and the resulting emergent behaviours.

MIL-STD-882E “Department of Defense - Standard Practice - System Safety” defines system safety as "the application of engineering and management principles, criteria, and techniques to achieve acceptable risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle" [12].

System safety engineering focuses on identifying and eliminating hazards, and minimizing risk where the hazards cannot be eliminated, with the ultimate goal of reducing the occurrence and severity of mishaps [12].

The system safety process in MIL-STD-882E consists of eight elements

[2] Emergent behavior of a system is behavior which is unexpected or cannot be predicted by knowledge of the system’s constituent parts. [10]

- Element 1: Document the System Safety Approach
- Element 2: Identify and Document Hazards
- Element 3: Assess and Document Risk
- Element 4: Identify and Document Risk Mitigation Measures
- Element 5: Reduce Risk
- Element 6: Verify, Validate and Document Risk Reduction
- Element 7: Accept Risk and Document
- Element 8: Manage Life-Cycle Risk [12]

An enterprise system consists of a purposeful combination of interdependent resources (e.g., people, processes, organizations, supporting technologies, and funding) that interact with 1) each other (e.g., to coordinate functions, share information, allocate funding, create workflows, and make decisions), and 2) their environment(s), to achieve business and operational goals through a complex web of interactions distributed across geography and time [10].

Two key concepts that are applied to deal with the complexities of enterprises are systems thinking and systems science. The primary characteristics of a systems approach are: (1) top-down systems thinking that recognizes safety as an emergent system property rather than a bottom-up, summation of reliable components and actions; (2) focus on the integrated socio-technical system as a whole and the relationships between the technical, organizational, and social aspects; and (3) focus on providing ways to model, analyze, and design specific organizational safety structures rather than trying to specify general principles that apply to all organizations." [13]

The complexity of an enterprise arises from its structural complexity, its dynamic complexity and its socio-political complexity. Structural complexity looks at the system elements and relationships. Dynamic complexity includes a time element and considers the complexity which can be observed when systems are used to perform tasks in an environment. Socio-political complexity considers the effects of individuals or groups of people on complexity. People-related complexity has two aspects. One is related to the perception of a situation as complex or not, due to multiple stakeholder viewpoints within a system context and social or cultural biases which add to the wider influences on a system context. The other involves either the "irrational" behavior of an individual or the swarm behavior of many people behaving individually in ways that make sense, however, the emergent behavior is unpredicted and perhaps counterproductive [10], [14].

System dynamics is an approach to understanding the behavior of complex systems over time. It deals with internal feedback loops and time delays that affect the behavior of the entire system [10]. System dynamics can be utilized to understand the challenges to safety over time due to social factors such as budget, schedule and lack of safety culture.

The main elements of System Dynamics are:

- The understanding of the dynamic interactions in a problem or solution as a system of feedback loops, modeled using a Causal Loop Diagram.
- Quantitative modeling of system performance as an accumulation of stocks (any entity or property which varies over time) and flows (representations of the rate of change of a stock).
- The creation of dynamic simulations, exploring how the value of key parameters change over time. A wide range of software tools are available to support this.

System dynamics models can be used to determine factors that will lead to increased risk over time, and then design features into the enterprise design to eliminate, control or mitigate those factors.

Cybernetics, the science of control, defines two basic control mechanisms:

- Negative feedback, maintaining system state against a set of objectives or levels.
- Positive feedback, forced growth or contraction to new levels [10].

"Socio-technical systems form what are known as control hierarchies, with systems at a higher level having some ownership of control over those at lower levels." [10] An enterprise modeled as a hierarchy of safety control structures can utilize some of the principles from cybernetics to achieve its safety goals.

"Separation of concerns describes a balance between considering parts of a system problem or solution while not losing sight of the whole" [10]. "Abstraction is the process of taking away characteristics from something in order to reduce it to a set of base characteristics" [10]. An iterative design process for the enterprise through stepwise refinement using models at increasing levels of detail will be the basis of the enterprise engineering process.

"Modeling is a common practice that is shared by most engineering disciplines, including:

- electrical engineering, which uses electrical circuit design models,
- mechanical engineering, which uses three-dimensional computer-aided design models, and
- software engineering, which uses software design and architecture models" [10].

Enterprise systems engineering (ESE) is the application of systems engineering principles, concepts, and methods to the planning, design, improvement, and operation of an enterprise

PDCA stands for "plan-do-check-act" and is a commonly used iterative management process. It is also known as the Deming circle or the Shewhart cycle after its two key proponents. ESE should use the PDCA cycle as one of its fundamental tenets [10].

Enterprise architecture frameworks are collections of standardized viewpoints, views, and models that can be used when developing architectural descriptions of the enterprise [10].

"The following four processes are needed in ESE beyond the traditional SE processes in support of enterprise management activities:

1. Strategic technical planning,
2. Capability-based planning analysis,
3. Technology and standards planning, and
4. Enterprise evaluation and assessment." [10]

While there is a body of knowledge in each of these areas individually, the integration of these concepts into a coherent approach to safety engineering at the enterprise level is not well covered by the literature.

Systems Theoretic Approach to Hazard analysis and Stepwise Refinement

A systems theoretic approach to hazard analysis contributes to the ability to manage the complexity of an enterprise to achieve its safety goals. It provides a means for hazard analysis of socio-technical systems that can be integrated into a stepwise refinement based approach to their design and evolution [2], [15].

Nancy Leveson has developed a Systems Theoretic Accident Model and Processes (STAMP) which provides a basis for a hazard analysis technique called

Systems Theoretic Process Analysis (STPA). STAMP focuses on identification and enforcement of safety constraints instead of identification and mitigation of failures. The three main concepts in the STAMP model are safety constraints, hierarchical control structures, and process models. By modeling a system using safety control structures at increasing levels of detail, a hazard analysis of each model can be performed that determines safety constraints on the behaviour of the system and its constituent elements necessary to avoid hazardous states of the system. Designing the system to enforce these safety constraints will deal with failures that result in hazardous states as well as hazardous states resulting from interactions between system elements. This approach to hazard analysis has the benefit of being able to deal with complex socio-technical systems, such as enterprises, where traditional hazard analysis techniques that focus on cause-effect failure chains are impractical to apply and ineffective for hazardous states resulting from interactions of system elements.

Another advantage of the STAMP based approach is that changes to the enterprise over time, especially during the operations phase of the enterprise, can be assessed for their impact on safety. Changes can introduce the need for new safety constraints, can modify previously identified safety constraints or can impact the effectiveness of design features originally introduced to enforce safety constraints. Once the safety impacts of changes are identified, the enterprise design can be modified to maintain the achievement of the enterprise's safety goals. System dynamics models can be utilized to identify sources of unsafe change, and then introduce design features that provide protection from these changes [2], [15].

Model of the Enterprise

The process of design inherently involves modeling of the system being designed and the various elements that make up the design. In a stepwise refinement based design process, the elements of the system can be designed in a recursive manner at incremental levels of detail [16]–[18].

A common reference model of the enterprise which defines the relevant components of the enterprise would provide a number of benefits. A common model would provide common terminology for the products to be designed from an enterprise design process. It would also permit the mapping of constructs and theories from the multiple disciplines that support enterprise engineering enabling

the definition of a coherent set of constructs and theories for enterprise engineering.

Defining the model to support various levels of abstraction of the representation of the enterprise will support the stepwise refinement process for the design of the enterprise.

A useful reference model will support hazard analysis, such as STPA, clearly reflect the Plan-Do-Check-Act process that is the basis of many management theories and provide guidance frameworks similar to that provided by many enterprise architecture frameworks. The model should be useful for performing organizational design, business process design, and design of governance structures since these can all have an impact on safety.

Nuclear Industry Best Practices

As a result of the Three Mile Island and Chernobyl nuclear accidents, the nuclear industry has established industry wide organizations to share best practices across all nuclear plants. Industry organizations such as INPO (Institute of Nuclear Power Operations) and IAEA (International Atomic Energy Agency) provide products and services to help nuclear operators improve their level of safety and incorporate lessons learned from other nuclear operators.

Figure 2 shows some of the key documents that capture nuclear industry best practice.

These documents are used by nuclear operators as a basis of assessments (self-assessments or by external assessors) to identify areas for improvement. The documents contain performance objectives, assessment criteria and best practices.

These industry documents are updated on a regular basis to reflect lessons learned over time. The Fukushima accident that occurred in Japan in 2011 is used as a basis to identify weaknesses in current practice in the nuclear industry against which to compare the SEE approach. IAEA documents have been updated after the Fukushima accident to reflect lessons learned. The SEE approach is also compared with these updated best practices.

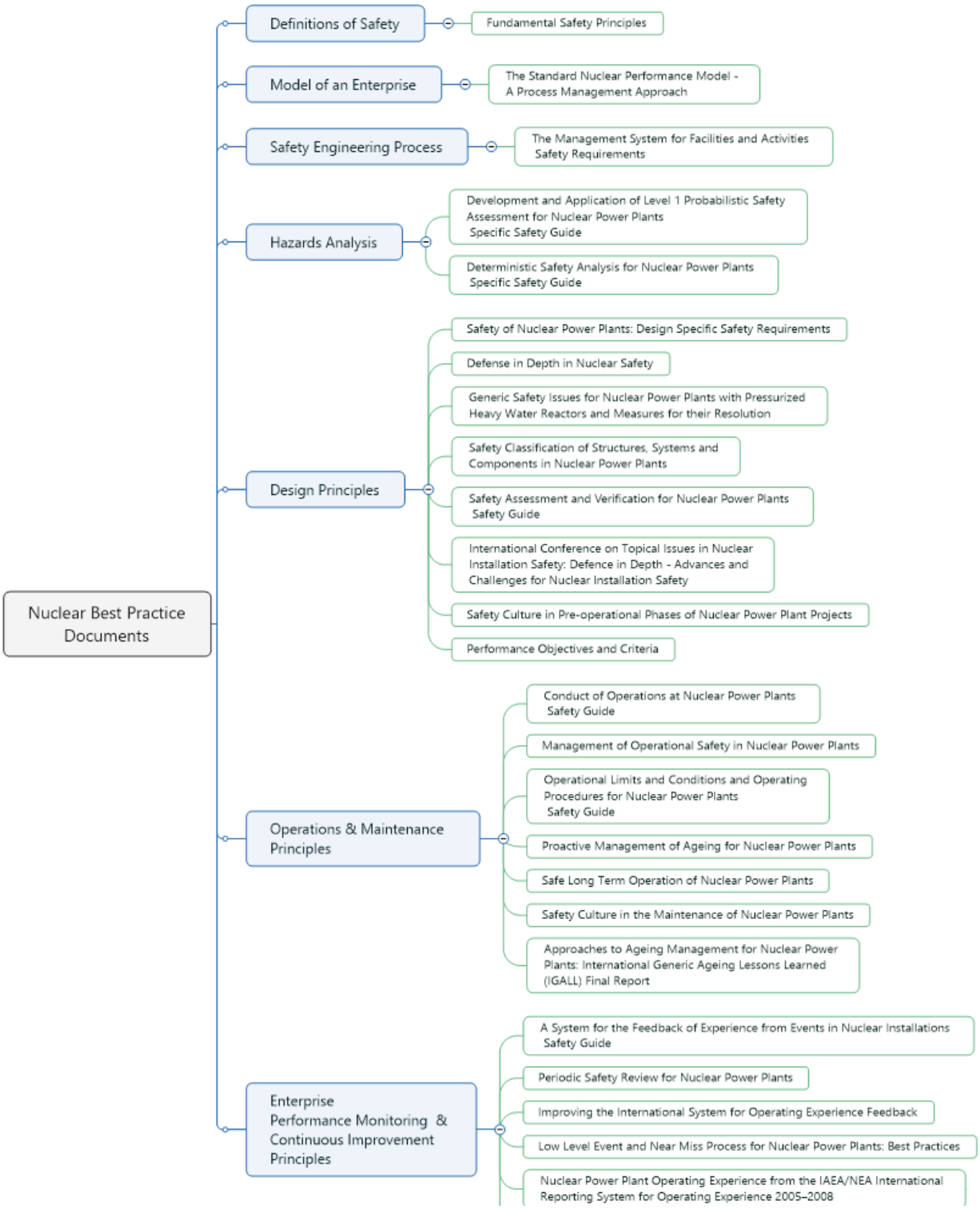


Figure 2 - Nuclear Industry Safety Practice Documents

3 RESEARCH METHODOLOGY

The scope of work in this thesis is to:

1) Define a Safety Enterprise Engineering (SEE) approach, and then
2) Assess whether the SEE approach is more effective at achieving safety goals than current practices in the nuclear power industry.

The definition of the SEE approach consists of the following steps:

- Definition of some foundational concepts related to safety, (Chapter 4)
- Definition of the safety enterprise engineering process, (Chapter 5)
- Definition of the hazard analysis process applicable to enterprise engineering, (Chapter 6) and
- Definition of a model of an enterprise to define the elements of the enterprise to be designed, (Chapter 7)
- Definition of principles that address typical classes of hazards by reviewing nuclear best practices and mapping them into the applicable portion of the enterprise design. (Chapter 8)

Figure 3 shows these steps graphically and some of the key outcomes of each step.

The assessment of the SEE approach within the nuclear power industry consists of the following steps:

- Use of the Fukushima Daiichi accident in 2011 to identify weaknesses with current practices within the nuclear industry, (Chapter 9)
- Use of IAEA best practices documents to identify weaknesses from Fukushima that are not well addressed by nuclear best practice documents including those documents updated to include lessons learned from Fukushima, (Chapter 10) and
- Application of the SEE approach to a slice of safety related functionality of a typical CANDU nuclear utility to assess the degree to which the SEE approach addresses weaknesses in current and best practices within the nuclear industry. (Chapters 11 and 12)

Figure 4 shows these steps graphically and some of the key outcomes of each step.

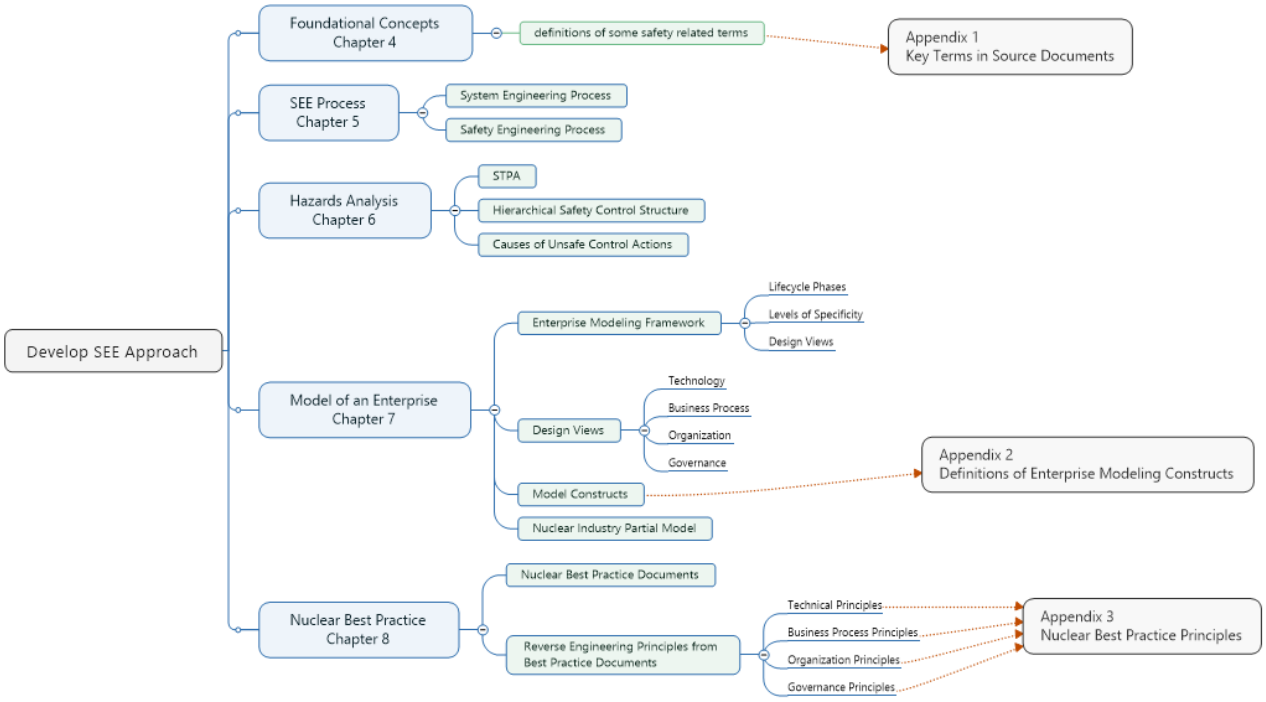


Figure 3 - Development of SEE Approach

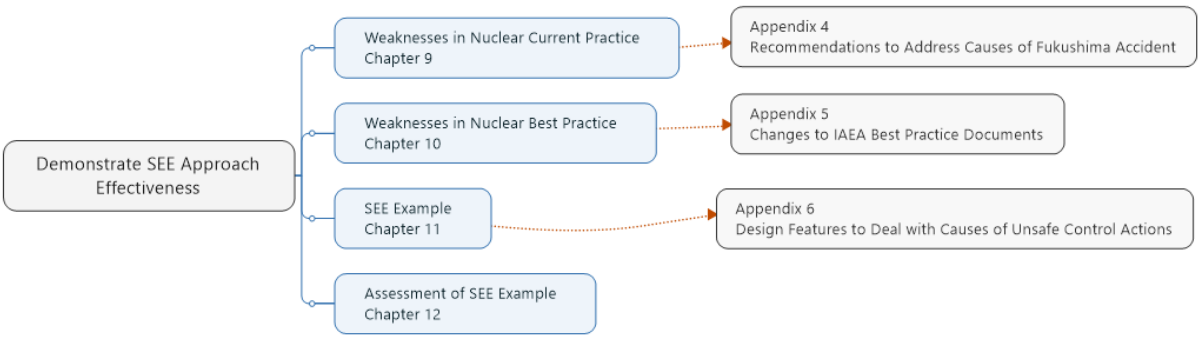


Figure 4 - Demonstration of SEE Approach Effectiveness

3.1 Definition of the Safety Enterprise Engineering Approach

To define the SEE approach, methods from the supporting disciplines of enterprise engineering, enterprise architecture, systems engineering, safety engineering and risk management were utilized. This involved extraction of key aspects of each discipline and integrating them together into a coherent engineering approach. Many others have done work in the various elements of the SEE approach, nobody has integrated them together into a coherent engineering approach as is reflected in the SEE approach. For example, Leveson has defined the STAMP model upon which the STPA hazard analysis method is based [2]. She also discusses safety-guided design and integrating safety into system engineering but does not integrate all these elements in to a coherent engineering approach.

As much as possible, industry standards within each discipline were used as source documents since they represent consensus on best practice within the scope of each standard.

The definitions of safety related terms were based on standards [11], [19], [20], [21], [22] and [12]. Reference [2] was also used since it represents some state of the art practices in hazard analysis for socio-technical systems.

The SEE process is based on the system engineering standard [23] and the risk management standard [24].

The definitions of the model of the enterprise is based on standards [25], [26], [27], [28]and [29] which deal with frameworks, concepts and descriptions of enterprise architectures.

The nuclear industry best practice principles were extracted from the IAEA documents listed in section 8.1.

The key contribution of the thesis is the extraction of the relevant aspects of each document above and their integration into a coherent approach that maintains a focus on achieving the overall safety goal.

Some of the key principles that the SEE approach is based upon are:

- Stepwise refinement in the design of the enterprise supporting analysis of the design at each level of detail in the refinement process;

- Keeping a clear distinction between requirements (what is required) versus design (how the requirements will be satisfied) at each level of refinement;
- Application of risk management at each level of refinement to identify hazards and incorporate design features necessary to achieve safety;
- Hazard analysis at each level of refinement that deals with the complexity inherent in a complex sociotechnical system such as an enterprise;
- Maintaining views of the design that allow analysis of the technologies, business processes, organizations and governance structures; and
- Reuse of the principles that are the basis of best practice in the nuclear industry to help identify potential causes of hazards and incorporate design features to deal with those hazards.

These principles are reflected in the SEE process, the artefacts resulting from the process and the guidance provided. The following sections elaborate on each principle.

3.1.1 Stepwise Refinement

Typically, complex systems are not engineered using a single pass of the system engineering technical processes. Enterprises, treated as the system to be engineered, are an example of a complex system. Stepwise refinement treats the overall system as a black box, for which the requirements are established. The black box is then broken down into a set of system elements. Each system element can be treated as a system and the process repeated until the system elements are simple enough to design without further refinement.

The system requirements definition process creates a set of requirements, including safety requirements. The architecture definition process defines an architecture (system elements and their interfaces) that satisfies the system requirements. If any element is considered too complex to design, then the element is treated as a system and the system requirements definition process and architecture definition processes are repeated until the element is simple enough to design without further refinement. Each set of system elements can then be integrated together to eventually realize the complete system.

Hazard analysis of the system architecture at each level of refinement can be performed to establish the safety requirements to be addressed by the architecture at the next level of refinement. At each level of refinement, it is also necessary to ensure that the architecture and/or design has not introduced new hazards that were not considered in any earlier hazard analysis.

At each level of refinement, the design can be viewed using the various design views discussed in section 3.1.5. Each design view focuses on different sets of design elements (which are related since they collectively make up the enterprise being engineered). The refinement process can result in the refinement of any of the elements represented in the design views (business processes, organizations, etc).

3.1.2 Requirements vs Design

Generally, a specification of "what" a system must do (requirements) is simpler than a specification of "how" the system will satisfy those requirements (architecture/design). Separation of requirements from architecture and design facilitates the exploration of various design alternatives and their ability to satisfy the requirements. This separation is of high value when dealing with complex systems such as an enterprise where there are many elements of the overall system with many interdependencies.

3.1.3 Risk Management

Risk management, in the context of safety management, is the set of activities to direct and control an organization to achieve its specified safety goals. Standards such as [24] define general risk management processes that must be instantiated for a specific context. The SEE approach integrates the general risk management process with the system engineering process of [23] to produce a safety engineering process that is applicable to enterprises.

At each level of refinement of the enterprise design, hazards are identified, analyzed and then design requirements/constraints are identified to eliminate, control or mitigate the hazards. The integration of risk management and systems

engineering with a stepwise refinement design process facilitates the early elimination, control and mitigation of risks. Traditional hazard analysis techniques are unwieldly when dealing with complex systems and hence are not effectively applied in practice.

3.1.4 Hazard analysis for Socio-technical Systems

Traditionally techniques for hazard analysis have been based on cause-effect chain models of accident causality. Cause-effect chain based techniques for hazard analysis are not effective for complex, socio-technical systems. STPA, or Systems-Theoretic Process Analysis, is a relatively new hazard analysis technique that bases its analysis on a safety control structure model of the system and hence is able to abstract away some of the underlying complexity.

The SEE approach incorporates STPA into its hazard analysis process by incorporating the safety control structure model in one of the design views of the enterprise being engineered.

Section 6.3 develops lists of generic, potential causes of unsafe control actions. These can be used as a checklist to help drive any specific hazard analysis being conducted using STPA.

3.1.5 Design Views

The design of the enterprise can be represented by different views that focus on specific aspects of the unified enterprise model that are prerequisite to achieving the safety objective. Four views used in the SEE approach are:

- the technology view,
- the business process view,
- the organizational view and
- the governance view.

These four views were selected since each represents aspects of the enterprise design that can lead to hazards and hence potentially accidents.

The technology view corresponds to the traditional scope of engineering efforts, where the boundaries of the system being engineered correspond to the boundaries of the technology whose behaviour can result in accidents.

The other views presented represent the aspects of the enterprise that can impact the technology and subsequently result in accidents.

Business processes define the activities that are undertaken to design, construct, operate, maintain, modify and decommission the technology. The business process view enables the representation and modification of the processes of the enterprise, their functionalities, behaviours, inputs and outputs. [26]. Inadequacies in business processes can lead to poor design, operation, maintenance or evolution of the technology and hence result in accidents.

The organizational view defines the organizational units, the organizational roles allocated to each unit and the skills required of people in those roles necessary to competently carry out the responsibilities of their role. Inadequacies in the performance of people in their roles can result in poor design, operations, maintenance or evolution of the technology and hence result in accidents.

Decision centres represent the decision making or governance roles within the enterprise. In this thesis the governance view will be represented as a "safety control structure" view to facilitate its usage in hazard analysis.

In systems theory, systems are viewed as hierarchical structures, where each level imposes constraints on the activity of the level beneath it- that is, constraints or lack of constraints at a higher level allow or control lower-level behavior. The safety control structure view is based on a feedback control system as a standardized structure for creating a hierarchical model of the enterprise. The safety control structure view is a useful representation for STPA based hazard analysis and represents the decision making or governance structures of the enterprise well. The safety control structure is very similar to management systems structures found in management science. The PDCA (plan, do, check, act) structure developed by Deming [30] is a structure common to many management systems and corresponds directly to the safety control structure.

The whole, integrated enterprise consists of all the elements reflected in each of these views.

3.1.6 Nuclear Best Practice Principles

The nuclear industry has a highly structured and comprehensive set of documents created and maintained by industry associations to capture and share best practices among nuclear industry utilities. The International Atomic Energy Agency (IAEA) is one such organization.

The principles and requirements in key IAEA documents associated with achieving safety of nuclear power plants were reviewed. For each principle/requirement an assessment was done to determine the underlying cause of hazard and design feature that the principle or requirement was derived from.

The list of causes of hazards and design features was organized by it applicability to the different lifecycle phases of a nuclear power plant and by which design view it primarily impacts. In this manner, the list can be used to help with the design and analysis of any specific nuclear power utility.

These industry documents are updated on a regular basis to reflect lessons learned over time. IAEA documents have been updated after the Fukushima accident to reflect lessons learned.

3.2 Assessment of the SEE Approach

To assess the effectiveness of the SEE approach weaknesses in current and best practice in the nuclear industry were identified, and then an example application of the SEE approach was performed to assess the degree to which the approach addressed the identified weaknesses.

The Fukushima nuclear accident that occurred in 2011 was used to identify weaknesses in current practices in the nuclear industry. These weaknesses were compared with best practices, as defined by IAEA documents, to identify the subset of weaknesses identified from the Fukushima accident that are also weaknesses within the IAEA set of best practices. The SEE approach was then applied to a slice of safety related functionality of a typical CANDU nuclear utility to demonstrate the degree to which the SEE approach overcomes weaknesses of both current practice and best practice.

3.2.1 Weaknesses in Current Nuclear Practices

The accident in 2011 at the Fukushima Daiichi nuclear power plant in Japan is one of the largest accidents in the history of nuclear power generation. The accident was analyzed by organizations in Japan, by industry organizations and by nuclear regulators internationally. The publicly available reports from these organizations were used to identify the recommendations for improvement to avoid future accidents due to the same underlying causes. This list of improvement recommendations is used in the thesis to represent weaknesses in current practice in the nuclear industry.

3.2.2 Weaknesses in Nuclear Best Practices

The list of current practice weaknesses, based on the Fukushima accident, was assessed against the principles/requirements in the set of IAEA best practice documents to determine the degree to which the IAEA documents address the weaknesses. Weaknesses for which there were not adequate principles/requirements are flagged as weaknesses in best practices.

Note that two key IAEA documents [31] and [32] were updated after the Fukushima accident and hence lessons learned from Fukushima should be reflected in them.

3.2.3 Application of SEE Approach to a Typical CANDU Nuclear Utility

To provide a basis against which to assess the SEE approach's ability to address the weaknesses in current and best practice within the nuclear industry, the SEE approach was applied to a slice of safety related functionality of a typical CANDU nuclear power utility.

The scope of the slice included both a technology function (steam generator level control) and a non-technology function (periodic safety review). The SEE approach was done at the overall enterprise level and then again at the steam generator level control and periodic safety review level. The analysis at the

overall enterprise level is constrained to only that portion that impacts the two lower level functions (steam generator level control and periodic safety review).

The scope of the slice was not adequate to cover all areas of weakness in current and best practice but was chosen to cover one technology related area and one non-technology area.

3.2.4 Assessment of Example

To assess the degree to which the example demonstrated the SEE approach's ability to address weaknesses in current and best practice, a set of criteria were established for each weakness against which the example was assessed. The criteria were identified by reviewing the details of each recommendation identified in Chapter 9 and identifying criteria that would reflect the successful implementation of the recommendation. The IAEA principles in Appendix 3 were also reviewed to identify criteria that are applicable to each recommendation.

Since the recommendations in Chapter 9 and the IAEA principles in Appendix 3 had to be analyzed and "criteria for the success of the SEE approach" distilled from that analysis, and since the author of this thesis developed the SEE approach and these criteria, it is quite possible that some sort of confirmation bias crept into this evaluation. With that in mind, the author developed the criteria before examining how the SEE approach would cope with the examples in the case study. Although this may not completely mitigate against confirmation bias, it would certainly help to constrain it. In addition, details of the individual steps are documented in the appendices, so that readers may determine for themselves whether or not confirmation bias likely affected the results.

The assessment concluded that each recommendation was either fully addressed, partially addressed, not addressed or that the scope of the example did not allow the recommendation to be assessed.

4 FOUNDATIONAL DEFINITIONS OF SAFETY

4.1 Introduction

A clear definition of safety is a prerequisite to defining an enterprise engineering approach to achieving and maintaining safety. The definition of safety varies amongst various safety related standards and between some key researchers in the area of safety. This Chapter will compare various definitions and then provide a consistent set of definitions of safety and the concepts upon which the definition of safety within the thesis is based. The definitions adopted within the thesis conform as closely as possible to generally accepted definitions reflected in international standards. The differences between the definition used in the thesis and the other sources of definitions are identified so that the reader can understand the relationships.

The thesis provides a risk based definition of safety along with definitions of terms such as risk, hazard, harm, and accident. Figure 5 shows some of the key safety related terms to be defined and their relationship to each other.

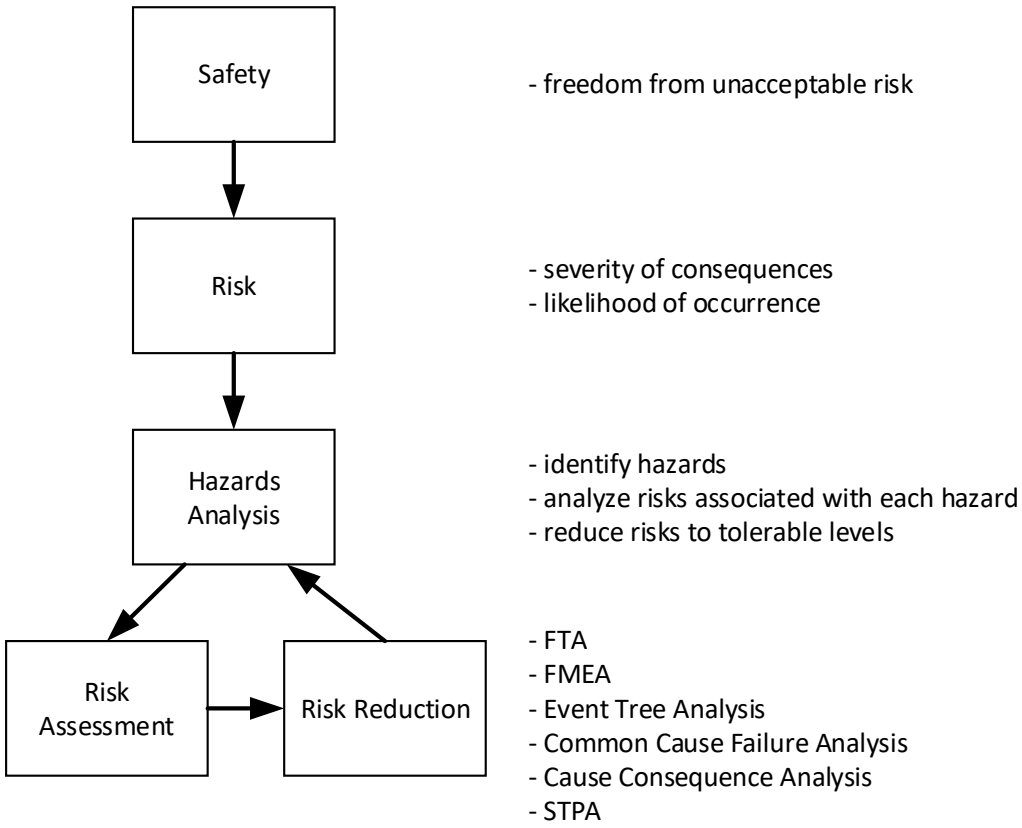


Figure 5 - Some Safety Related Terms

The following sections provide a set of definitions of some key safety related terms that will be used in this thesis. The definitions are based on the following safety related standards:

- ISO/IEC Guide 51 - Safety aspects – Guidelines for their inclusion in standards [11]
- ISO/IEC 15026-3 - Systems and software engineering - Systems and software assurance - Part 3: System integrity levels [20]
- IEC 61508-4 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations [19]
- ISO 26262-1 Road vehicles — Functional safety — Part 1: Vocabulary [19]
- MIL-STD-882E - Department of Defense Standard Practice - System Safety [12]

- IEC 61226 Ed.3: Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions. [33]
- IAEA Safety Glossary - Terminology Used in Nuclear Safety and Radiation Protection [22]

The safety related terms used in the book "Engineering a Safer World" by Nancy G. Leveson [2] are also considered since concepts from her book are used for hazard analysis within the thesis.

Appendix 1 summarizes the key terms defined in each of the above safety related standards and their relationships.

4.2 Safety

SAFETY: freedom from unacceptable risk

This is the definition used in ISO/IEC Guide 51 and IEC 61508. Table 1 shows the definitions of safety from all the source standards.

Source Document	Definition of Safety
ISO/IEC Guide 51	Freedom from unacceptable risk
IEC 61508	Freedom from unacceptable risk
ISO/IEC 15026-3	Tolerable risk (in the safety context)
ISO 26262	Absence of unreasonable risk
IAEA Safety Glossary	'safety' means the protection of people and the environment against radiation risks, and the safety of facilities and activities that give rise to radiation risks.
MIL-STD-882E	Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Engineering a Safer World	Freedom from accidents (loss events)

Table 1 - Definitions of Safety

Most of the definitions are risk based and are equivalent. The two exceptions are the definitions from MIL-STD-882E and from Leveson, which do not include a risk based aspect of safety. Those two sources define safety as being freedom from accidents. In most circumstances there will be some probability of accidents occurring. In these circumstances "safety" is not achievable if safety is defined as the "absolute" freedom from accidents occurring. In general, a judgement must be made on the acceptability of the risk remaining after all reasonable risk reduction measures have been taken.

In MIL-STD-882E, the scope of the standard is stated to be: "This system safety standard practice identifies the Department of Defense (DoD) Systems Engineering (SE) approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated." So even though its definition of safety does not directly involve risk, the intent of the standard is the same as a risk based approach in that it strives to eliminate hazards if possible, and otherwise to "minimize risks". This does not clearly state that the goal is to minimize the risk to an acceptable level, but it is implied.

MIL-STD-882E does define "System Safety" as "The application of engineering and management principles, criteria, and techniques to achieve acceptable risk within the constraints of operational effectiveness and suitability, time, and cost throughout all phases of the system life-cycle". Hence it acknowledges the concept of "acceptable risk" in its definition of system safety.

Leveson defines concepts of "Hazard Level" and "Risk Level" that are consistent with a risk based approach to safety. The concern that Leveson has with a risk based approach to safety is reflected in the following extract from her book on Engineering a Safer World:

"Understanding risk is important in decision making. Many people assume that risk information is most appropriately communicated in the form of a probability. Much has been written, however, about the difficulty people have in interpreting probabilities. Even if people could use such values appropriately, the tools commonly used to compute these quantities, which are based on computing probabilities of failure events, have serious limitations. An accident model that is not based on failure events, such as the one introduced in this book, could provide

an entirely new basis for understanding and evaluating safety and, more generally, risk."

So Leveson acknowledges a risk based approach, but qualifies it based on an appropriate approach that deals with the limitations of "computing probabilities of failure events".

The thesis will continue with the intent of defining a safety management approach that achieves "acceptable risk" but takes into account the limitations of computing probabilities of failure events, as noted by Leveson.

4.3 Risk

RISK: combination of the probability of occurrence of harm and the severity of that harm

This definition of risk is consistent across all the source documents.

4.4 Unacceptable Risk

UNACCEPTABLE RISK: risk judged to be unacceptable in a certain context according to valid societal moral concepts

This definition is from ISO 26262. The definitions in the various source documents are consistent. Many chose to define acceptable or tolerable risk instead of unacceptable risk. Table 2 lists the definitions from the source documents for unacceptable risk (or equivalent terms).

Source Document	Definition of Unacceptable Risk (or equivalent term)
ISO/IEC Guide 51	**Tolerable risk**: risk which is accepted in a given context based on the current values of society.
IEC 61508	**Tolerable risk**: risk which is accepted in a given context based on the current values of society.
ISO/IEC 15026-3	**Tolerable risk**: level of risk that is accepted in a given context based on the current values of society
ISO 26262	**Unreasonable risk**: risk judged to be unacceptable in a certain context according to valid societal moral concepts
IAEA Safety Glossary	**Unacceptable consequence**: consequence of an operational state or a PIE (postulated initiating event), that exceeds specified limits for the corresponding plant states, in terms of releases at the site or the wider environment.[3]
MIL-STD-882E	**Acceptable risk**: Risk that the appropriate acceptance authority is willing to accept without additional mitigation.
Engineering a Safer World	**Risk Level**: A function of the hazard level combined with (1) the likelihood of the hazard leading to an accident and (2) hazard exposure or duration. **Hazard Level**: A function of the hazard severity (worst case damage that could result from the hazard given the environment in its most unfavorable state) and the likelihood (qualitative or quantitative) of its occurrence.

Table 2 - Definitions of Unacceptable Risk (or equivalent terms)

[3] Definition is from IEC 61226 "Nuclear Power Plants – Instrumentation and control important to safety – Classification of instrumentation and control functions"

4.5 Hazard

HAZARD: A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident.

Table 3 shows the definitions of hazards from the source documents. The thesis will use the definition from Leveson because it makes explicit the aspects of the "state of the system" and the "state of the environment" that together lead to an accident. The other definitions (potential source of harm) are consistent with this definition but do not highlight the state of the system vs the state of its environment, which I believe are important aspects to highlight.

Source Document	Definition of Hazard
ISO/IEC Guide 51	Potential source of harm
IEC 61508	Potential source of harm
ISO/IEC 15026-3	**dangerous condition:** state of a system which, in combination with some states of the environment, will result in adverse consequence Note 1 to entry: A hazardous situation in ISO/IEC Guide 51 and IEC 61508–4 is an instance of a dangerous condition. A concept of dangerous conditions is introduced in order to cover not only hazardous situations in the safety context but also errors in the reliability, integrity, confidentiality, or dependability contexts and other states of a system which can lead to adverse consequences.
ISO 26262	Potential source of harm caused by malfunctioning behaviour of the item
IAEA Safety Glossary	Hazard is not defined in the IAEA Safety Glossary. The following definition comes from the Office for

	Nuclear Regulation in the UK "Guide to Nuclear Regulation in the UK: a hazard is any source that has the potential to cause harm
MIL-STD-882E	A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
Engineering a Safer World	A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss).

Table 3 - Definitions of Hazard

4.6 Harm

HARM: physical injury or damage to the health of people, or damage to property or the environment

This definition is from ISO/IEC Guide 51. It is consistent with the other source documents except for ISO 26262 which restricts the definition of harm to "physical injury or damage to the health of persons".

4.7 Accident

ACCIDENT: An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on).

The above definition comes from Leveson's "Engineering a Safer World". The term "accident" is not used in all the source documents but there are equivalent terms for accident, such as "harmful event", "hazardous event", "adverse consequence" or "mishap" that are defined and have equivalent meaning. Table 4 provides the various definitions from the source documents.

Source Document	Definition of Accident (or equivalent term)
ISO/IEC Guide 51	**Harmful event**: occurrence in which a hazardous situation results in harm
IEC 61508	**Hazardous Event**: event that may result in harm
ISO/IEC 15026-3	**Adverse Consequence**: consequence that results in a specified level of loss. Note 1: An adverse consequence results from the system-of-interest being in a dangerous condition combined with the environment of the system being in its worst-case state (relative to the adverse consequence). Note 2: Harm in ISO Guide 51 is an instance of an adverse consequence. The concept of adverse consequences is introduced in order to cover not only harm in the safety context but also other losses such as loss of assets in the security context.
ISO 26262	**Hazardous Event**: combination of a hazard and an operational situation
IAEA Safety Glossary	Any unintended event, including operating errors, equipment failures and other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.
MIL-STD-882E	**Mishap**: An event or series of events resulting in unintentional death, injury, occupational illness,

	damage to or loss of equipment or property, or damage to the environment.
Engineering a Safer World	An undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on).

Table 4- Definitions of Accident (or equivalent term)

5 SAFETY ENTERPRISE ENGINEERING PROCESS

The Safety Enterprise Engineering (SEE) process will result in the definition of an enterprise design, including the technology, organizational design, governance structure and business process design that is intended to achieve the enterprise's safety goals.

Three key principles that the SEE process is based upon are:

- Stepwise refinement in the design of the enterprise supporting analysis of the design at each level of detail in the refinement process
- Keeping a clear distinction between requirements (what is required) versus design (how the requirements will be satisfied) at each level of refinement
- Application of risk management at each level of refinement to identify hazards and incorporate design features necessary to achieve safety

As described in section 7.1.1, there are three lifecycle phases for the enterprise;

1. design and construction phase,
2. operations and maintenance phase, and
3. decommissioning phase.

The SEE process must define the design of the dangerous technology[4] and build it during the design and construction phase consistent with the enterprise's safety goals. The process must also define the organizational design and business process design used during all three phases to achieve, and maintain achievement of, the enterprise's safety goals.

Section 5.1 defines the approach to engineering the enterprise based on systems engineering practices. Section 5.2 defines the safety engineering approach to achieve the safety goal, and its integration into the safety enterprise engineering process. Section 5.3 describes how protection from degradation of safety over time can be achieved.

The process reflects the iterative risk management process of hazards identification and design to deal with hazards. The safety control structure view of the enterprise is used to support hazard analysis using a technique called STPA

[4] Dangerous technology is a technology that has some safety concerns associated with it

which is able to cope with the complexity associated with organizational and business process design.

The safety control structure view also has the benefit of being able to isolate the decision making elements of the design so that safety culture attributes can be identified for various decisions made at different levels within an organization.

The process is defined in a manner that supports its recursive application during a stepwise refinement design process.

5.1 System Engineering Process

The process used to engineer a system is well defined within standards such as ISO/IEC/IEEE 15288 [23]. These standards define the technical processes for systems engineering as well as the technical management processes, organizational project enabling processes and agreement processes necessary to engineer a system. Figure 6 shows the system engineering processes defined in ISO/IEC/IEEE 15288 [23].

In the context of safety enterprise engineering, the scope of the system being engineered can be considered to be the entire enterprise including the dangerous technology and the enterprise's business processes and organizations that design, construct, operate, maintain and decommission the dangerous technology.

The technical processes reflect the application of stepwise refinement through recursive application of the system requirements definition process and the architecture definition process until system elements in the architecture are simple enough to design without further refinement. These system elements are then designed, implemented, and integrated together to produce the complete system.

The key technical processes in ISO/IEC/IEEE 15288 [23] are as follows.

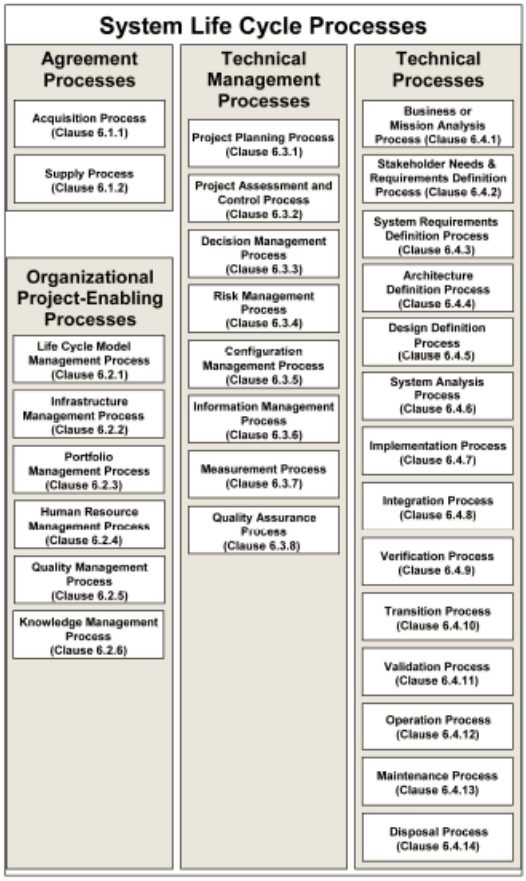


Figure 6 - ISO/IEC 15288 System Engineering Processes [23]

5.1.1 Systems Requirements Definition

This process creates a set of measurable system requirements that specify what characteristics, attributes, and functional and performance requirements the system is to possess, in order to satisfy stakeholder requirements.

In the context of safety enterprise engineering, the requirements must include:

- definition of the accidents to which the enterprise could contribute,
- definition of the system boundaries, so that elements outside the enterprise scope are identified, especially if they can contribute to the accident,
- system hazards, so that the potential role of the enterprise contribution is commonly understood, and
- system safety requirements necessary to achieve the safety goal.

5.1.2 Architecture Definition

The architecture definition process defines an architecture (system elements, their interfaces and interconnections) that satisfies the system requirements.

Architecture definition may be applied at many levels of abstraction, highlighting the relevant detail that is necessary for the decisions at that level. Typically, a stepwise refinement process is used. If any element of the architecture is considered too complex to be designed, then the element is treated as a system and the system requirements and architecture definition processes are repeated until elements that are simple enough to be designed are defined. Figure 7 illustrates a simple example of a case where element 2 was considered too complex and, hence, further refined.

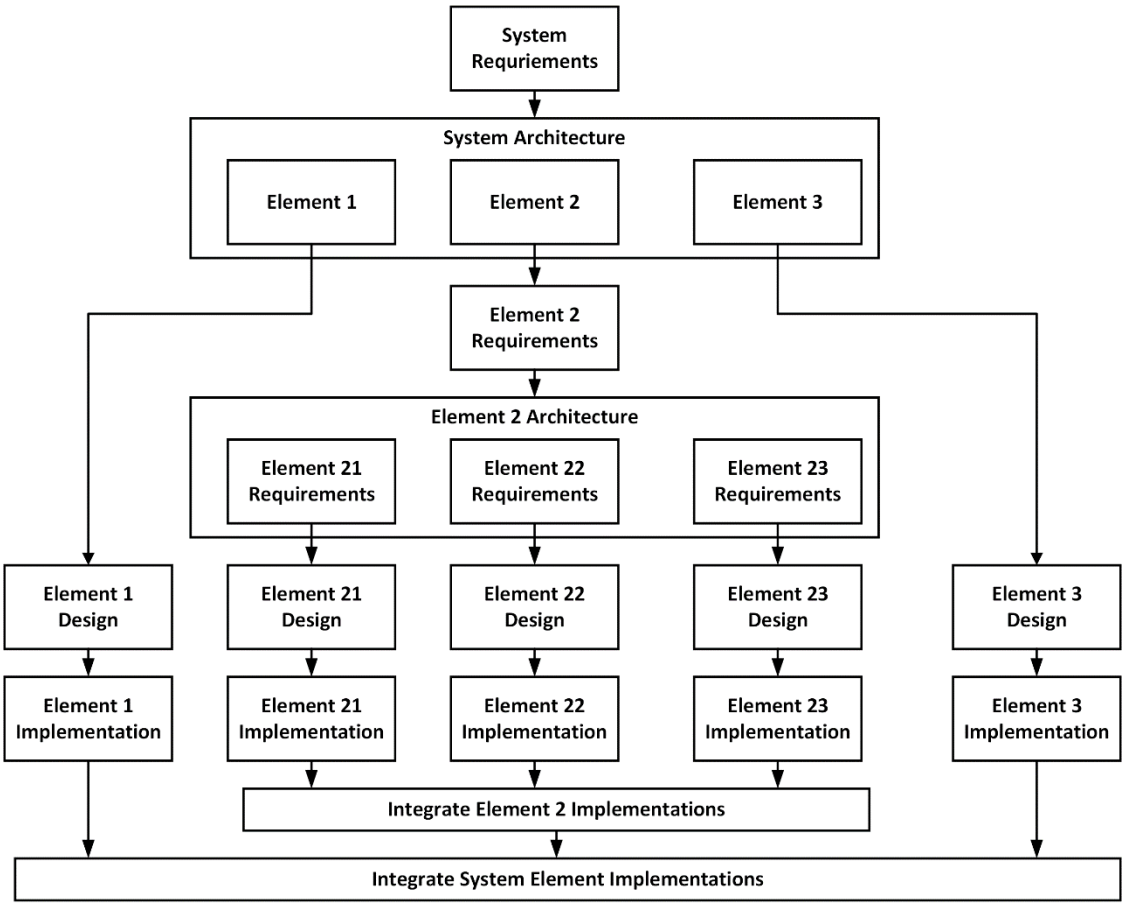


Figure 7 - Simple Example of Stepwise Refinement Process

5.1.3 Design Definition

"The purpose of the Design Definition process is to provide sufficient detailed data and information about the system and its elements to enable the implementation consistent with architectural entities as defined in models and views of the system architecture" [23].

5.1.4 Implementation

"The purpose of the Implementation process is to realize a specified system element" [23].

5.1.5 Integration

"The purpose of the Integration process is to synthesize a set of system elements into a realized system (product or service) that satisfies system requirements, architecture, and design" [23].

For a given level of the system hierarchy, this process iteratively combines implemented system elements to form complete or partial system configurations in order to build a product or service. It is used recursively for successive levels of the system hierarchy.

5.1.6 Operation

"The purpose of the Operation process is to use the system to deliver its services" [23]. To be safe, the system must be operated within the safe operating envelope established during the design of the system. The safe operating envelope refers to the set of limits and conditions within which the system must be operated to ensure conformance with the safety analysis.

5.1.7 Maintenance

"The purpose of the Maintenance process is to sustain the capability of the system" [23]. Corrective maintenance must be performed in a timely manner in order to achieve availability[5] requirements established during the design of the system. Preventive maintenance must be performed with sufficient frequency to maintain compliance with reliability targets established during the design of the system.

5.2 Safety Engineering Process

The engineering of a system where there are safety concerns involves safety engineering. Safety engineering involves managing the safety risks of the system by identifying system hazards, identifying how the system hazards can occur, and then modifying the architecture or design of the system to either eliminate, control or mitigate the hazards. This risk management process must be applied at each level of refinement to identify hazards and incorporate design features necessary to achieve safety. The approach to hazard analysis at each level of refinement must deal with the complexity inherent in a complex sociotechnical system such as an enterprise. Figure 8 shows the relationships between risk management and systems engineering that achieves safety using the processes in [24] and [23].

One advantage of the SEE approach over traditional safety engineering approaches is in how probabilities and the ALARA (as low as reasonably achievable) principle are applied. In traditional safety engineering approaches, hazard identification (and subsequent risk reduction) does not include what are assessed to be very low probability events. The SEE approach identifies all causes of unsafe control actions independent of any assessment of their probability of occurrence. Of course, any specific design cannot typically incorporate design features that deal with every possible cause of unsafe control actions to the point where the likelihood of an accident is zero. The "reasonably achievable" aspect of ALARA will still come into play, but, by allowing all events to be analyzed, the reasonability of corresponding design features can be

[5] Availability is a measure of the percentage of time that a system is available to perform its specified function. Availability is determined by the failure rate of a system, the time it takes to detect the failure and the time it takes to repair the system after failure.

assessed. Some design features will be reasonable to implement despite the fact they may address very low probability events.

The key difference is that traditional approaches eliminate certain events from consideration due to their low probability of occurrence. The SEE approach considers all events that can lead to hazardous states and only eliminates design features if they are considered "unreasonable". Unreasonable includes eliminating design features that are expensive to implement and only deal with low probability events.

This approach also eliminates the need to make assumptions on the probability of occurrence for events that may have a very weak basis for establishing the probability of occurrence, as is the case with complex socio-technical systems.

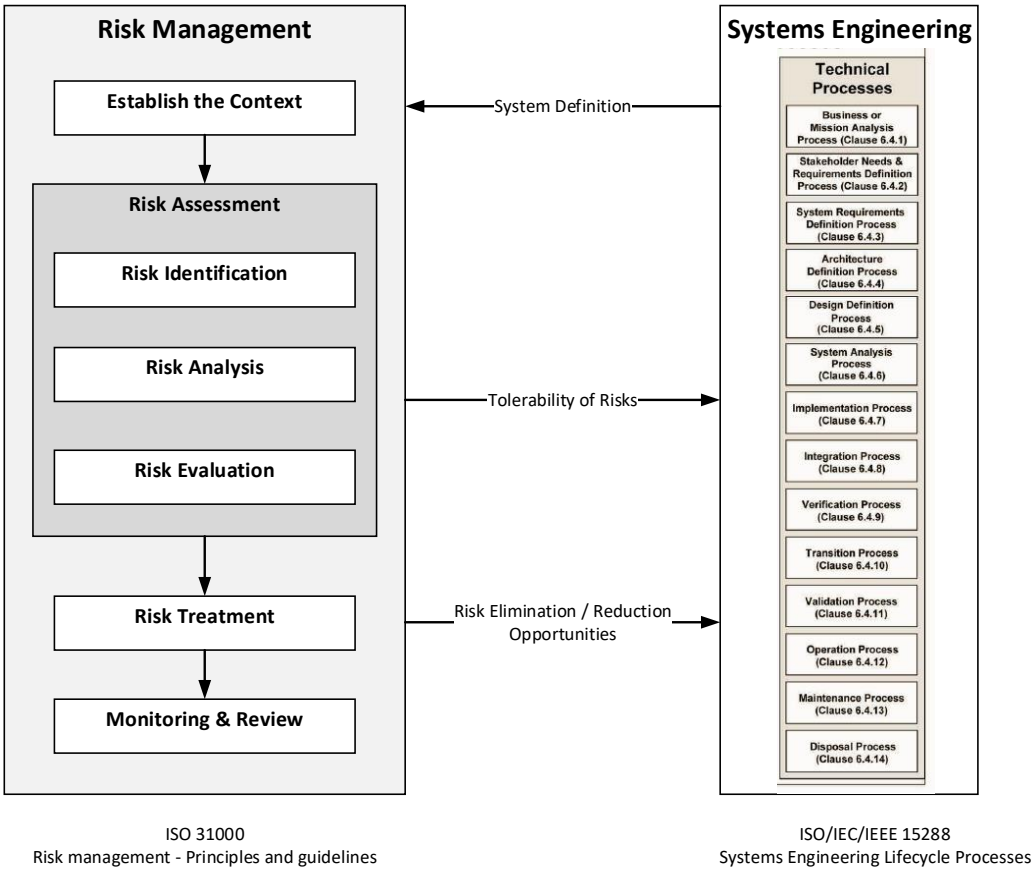


Figure 8 - Safety Engineering Process

5.3 Causes of Degradation of Safety Over Time

The design features that control or mitigate causes of hazards can degrade over time through modifications to the technological system, changes to the operations, maintenance and modification processes, or due to changes in the organizations and capabilities of the people over time.

Ongoing monitoring of the performance of the technological systems, business processes and organization must be done to detect non-compliances with safety requirements and enact corrective actions where necessary. These processes are part of a continuous improvement program that strives to maintain safety risks as low as practically achievable.

Ongoing monitoring of the environment of the enterprise is also necessary. This includes monitoring of changes to:

- regulatory, legal and societal expectations with respect to the definition of tolerable risk (i.e. safety) and
- the understanding of the behaviour of systems in the environment (natural and engineered systems).

When changes to the above are detected then an assessment must be done to determine if changes are required to the enterprise to maintain achievement of safety.

These performance monitoring and continuous improvement processes are part of each management process defined in [23] and shown in Figure 6.

6 HAZARD ANALYSIS

As described in Chapter 5, one of the key steps in achieving safety is to identify hazards, evaluate the impact of the hazards on safety and then determine changes to the architecture or design of the system to either eliminate, control or mitigate the cause of the hazard.

Traditionally, techniques for hazard analysis have been based on cause-effect chain models of accident causality. These techniques identify hazards based on identifying cause-effect chains from component failures to system level hazards. These techniques are based on reliability engineering and deal with component failures. Traditional hazard analysis techniques include Failure Modes and Effects Analysis (FMEA), and Fault Tree Analysis (FTA).

These cause-effect chain models were extended to include human error as factors that lead to failures that lead to accidents. Figure 9 shows Heinrich's Domino Model of Accidents that shows that unsafe failures can be the result of human error, which in turn can result from social environmental factors [34]. Figure 10 shows the Reason's Swiss Cheese Model of Accidents [35] which represents the same factors but with the social environmental factors shown in more detail as different types of latent failures. The unsafe act that leads to an accident is a result of cascading failures of all the defenses.

Cause-effect chain based techniques for hazard analysis are not effective for complex, socio-technical systems. "Accident models and explanations involving only simple chains of failure events can easily miss subtle and complex couplings and interactions among failure events and omit entirely accidents involving no component failure at all." [2] STPA, or Systems-Theoretic Process Analysis, is a new hazard analysis technique that bases its analysis on a safety control structure model of the system and hence is able to abstract away some of the underlying complexity. STPA identifies safety constraints that the system must satisfy which can then be used as input to the system engineering process. This approach therefore envelopes the required safe behaviour of the system without having to identify every cause-effect chain that can result in a hazardous state of the system.

This Chapter, Chapter 6, provides

- an introduction to hazard analysis (section 6.1),
- a description of STPA hazard analysis (section 6.2), and

- a description of generic causes of unsafe control actions based on analysis of the safety control structure model upon which STPA is based (section 6.3).

6.1 Introduction to Hazard analysis

Recall from section 4.5 that a hazard is defined as "A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident.". Hazard analysis is focused on identification of those hazardous system states or sets of conditions (hazards) so that the causes of the hazards can be identified and design features to eliminate, control or mitigate the causes can be incorporated in the design.

FMEA is a bottom-up approach that examines component failures and determines if the cause-effect chain from the component failure will lead to a hazard. FTA is a top down technique that starts from identified hazards and then determines what cause effect chains can result in the hazard.

For component failures that lead to hazards, design features such as use of highly reliable components, or use of redundancy can be used to reduce the likelihood of the failure and hence increase safety. It may also be possible to mitigate the consequences of the failure by design features that detect the failure and put the system into a safe state and thereby avoid the hazard.

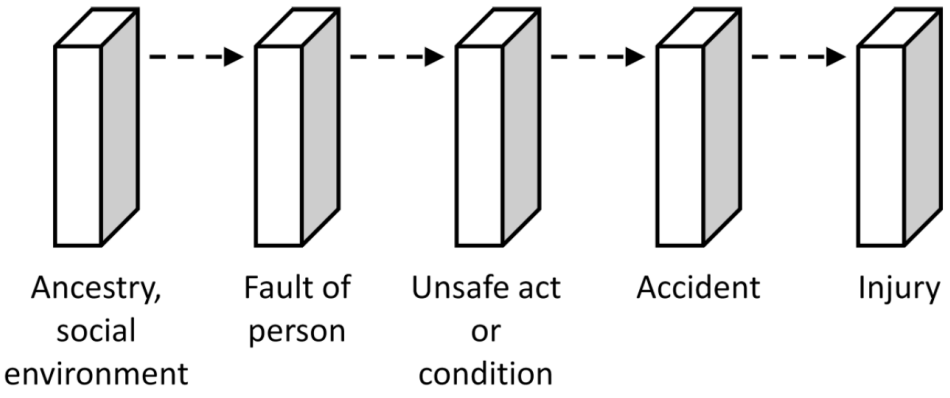


Figure 9 - Heinrich's Domino Accident Model [34]

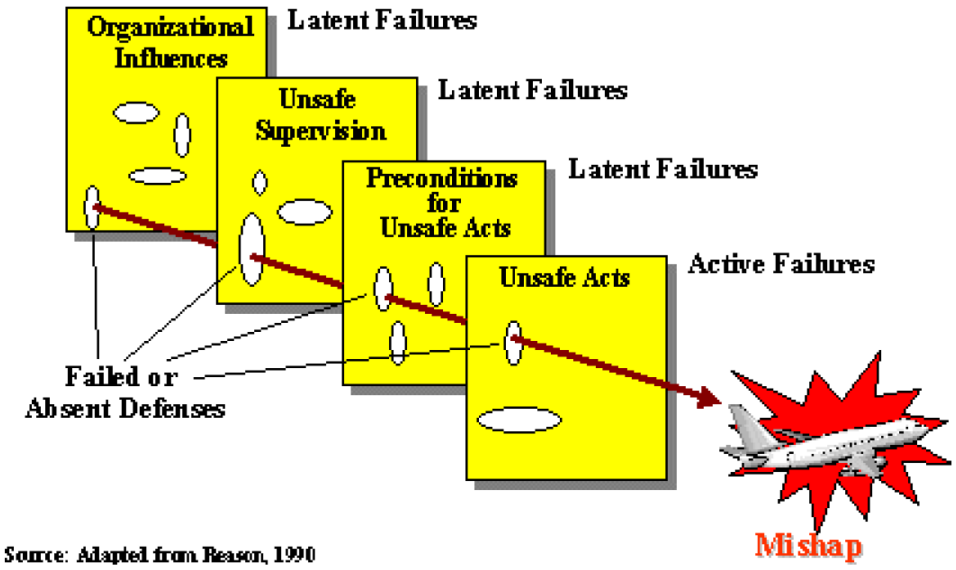


Figure 10 - Reason's Swiss Cheese Model of Accidents [35]

There are a few challenges to effective use of these traditional hazard analysis techniques with complex, socio-technical systems.

Firstly, the number of component or human failures for consideration is large making the hazard analysis effort onerous, if not infeasible. This results in the hazard analysis being expensive and time consuming to both produce and maintain over the life of the system.

Secondly, often hazards result from combinations of failures. The combinations of component failures and human error is very large and hence cannot be effectively analyzed using techniques that require the enumeration of each cause effect chain that can result in a hazard. The results of hazard analysis is limited by experts' ability to recognize all relevant phenomena, including potentially important external hazards, and by uncertainties and incompleteness of estimates of accident probabilities and consequences.

Thirdly, in complex systems, hazards can result from unintended interactions between system elements and hence are not caused by any failures of system

elements. Hence techniques that focus solely on identification of failures are ineffective at finding this class of causes of hazards.

To overcome these limitations of traditional hazard analysis techniques, STPA approaches the analysis from a different perspective. STPA identifies safety constraints that must be enforced in order to avoid hazards. The analysis then identifies causal factors that could challenge the enforcement of the safety constraints. Design features to eliminate, control or mitigate those casual factors can then be included in the design of the system. STPA is based on analysis of a hierarchical safety control structure model of the system. Hazards come about due to inadequate enforcement of safety constraints on the hazardous process behaviour, as shown in Figure 11.

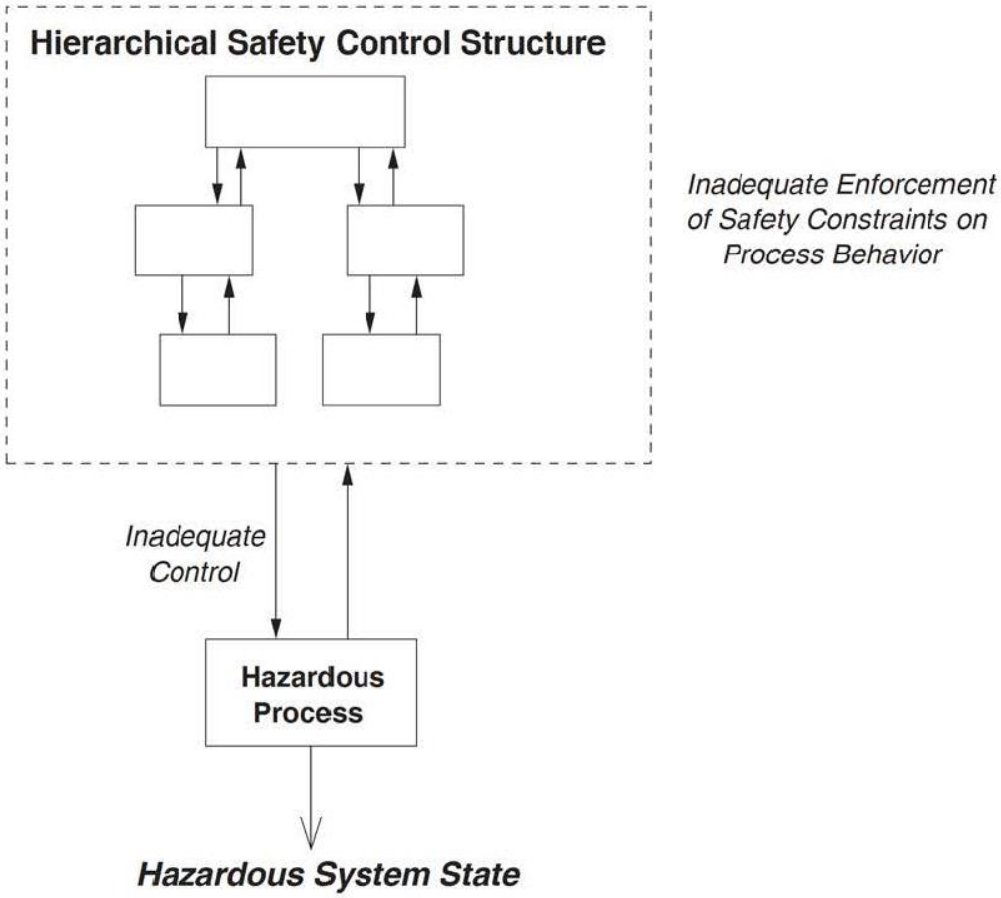


Figure 11 - Accidents Result from Inadequate Enforcement of Behavioural Constraints [36]

Analysis based on this abstracted model of the system allows causal factors beyond just component or human failures to be identified. The next section describes the STPA process in more detail.

6.2 STPA

"STPA, or Systems-Theoretic Process Analysis, is a new hazard analysis technique with the same goals as any other hazard analysis technique, that is, to identify scenarios leading to identified hazards and thus to accidents so they can be eliminated or controlled. STPA, however, has a very different theoretical basis or accident causality model. STPA is based on systems theory while traditional hazard analysis techniques have reliability theory at their foundation.

While traditional techniques were designed to prevent component failure accidents (accidents caused by one or more components that fail), STPA was designed to also address increasingly common component interaction accidents, which can result from design flaws or unsafe interactions among non-failing (operational) components. In fact, the causes identified using STPA are a superset of those identified by other techniques." [36]

The STPA process can be separated into seven parts, although the various activities could be intertwined and, in the most effective uses, STPA becomes the stepwise refinement engineering process with detail added as the system design evolves. The STPA analysis is based on a safety control structure model of the system that reflects the stage of design at the time of the analysis.

The seven steps are as follows:

1) Establish the system engineering foundation for the analysis and for the system development (accidents or losses to be considered, hazards associated with these accidents, safety requirements, and the safety control structure)

2) Identify potentially unsafe control actions based on analysis of the safety control structure

3) Use the identified unsafe control actions to create safety requirements and constraints

4) Augment the safety control structure with details of the controllers' process models (the controller's process model is defined to determine the environmental and system states that affect the safety of the control actions)

5) Determine how each potentially hazardous control action could occur. This step in the analysis identifies scenarios that can lead to:

    a. the unsafe control actions, that is, the hazards, including the causes of the process model being incorrect
    b. A required (safe) control action being given but not executed. Note that the results here will include the traditional failure analysis (e.g., FTA, HAZOP, FMECA) results

6) Incorporate design controls/features/constraints to eliminate, control or mitigate the hazards based on the identified possible causes

7) Consider how the designed controls/features/constraints could degrade over time and build in protection

Step 2, the identification of unsafe control actions, utilizes the fact that there are four general types of unsafe control action [36]:

1) An unsafe control action is provided that creates a hazard
2) A required control action is not provided to avoid a hazard
3) A potentially safe control action is provided too late, too early, or in the wrong order
4) A continuous safe control action is provided too long or is stopped too soon

6.3 Causes of Unsafe Control Actions

This section identifies generic causes of unsafe control actions based on analysis of the safety control structure. The generic causes identified incorporate work from [2], [37] and [38].

"A hierarchical safety control structure is an instance of the more general system theory concept of hierarchical control structure. The goal of the safety control structure (sometimes called the safety management system) is to enforce safety constraints and therefore eliminate or reduce losses." [36]

One advantage of the analysis based on the safety control structure representation is that generalized causal factors for failing to enforce the safety constraints can be identified and then used to analyze the specific safety control structure for the system being analyzed. Figure 12 shows these generalized sources of causes of failures for a simple safety control structure representation.

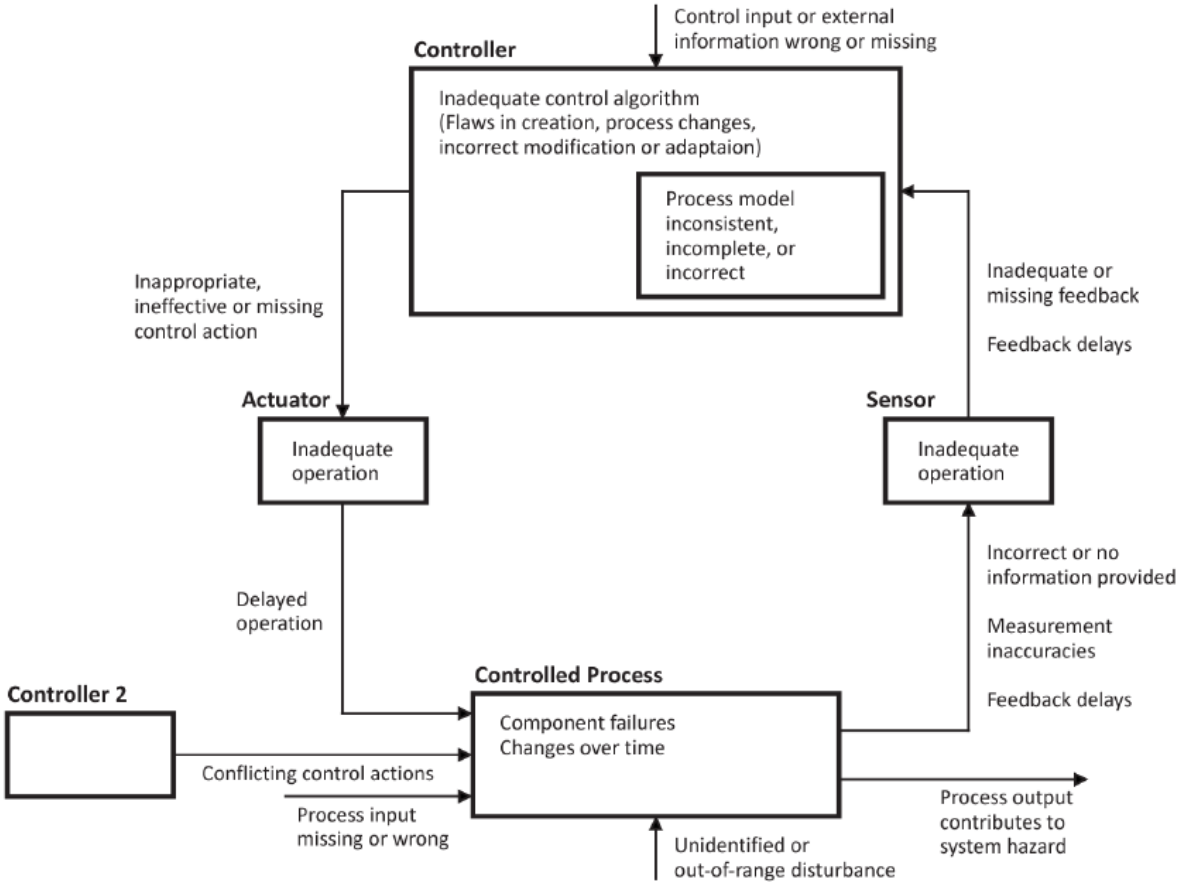


Figure 12 - Potential Sources of Hazards [2]

The analysis is sensitive to the safety control structure model used. Since the safety control structure is an abstract representation of the system, it is possible that the details that have been left out will impact the results of the analysis of the model. Knowledgeable analysts and the application of hazard analysis at each stage of stepwise refinement, as details are added, helps to mitigate this concern. Section 7.3.4 discusses the creation of safety control structure models of the system.

"Figure 13 shows an example for a typical regulated industry. Between each level there is a feedback control loop as defined in system theory. Higher level controllers may provide overall safety policy, standards, and procedures, and get feedback about their effects in various types of reports, including incident and accident reports. Lower levels implement those policies and procedures. Feedback

provides the ability to learn and to improve the effectiveness of the safety controls." [36]

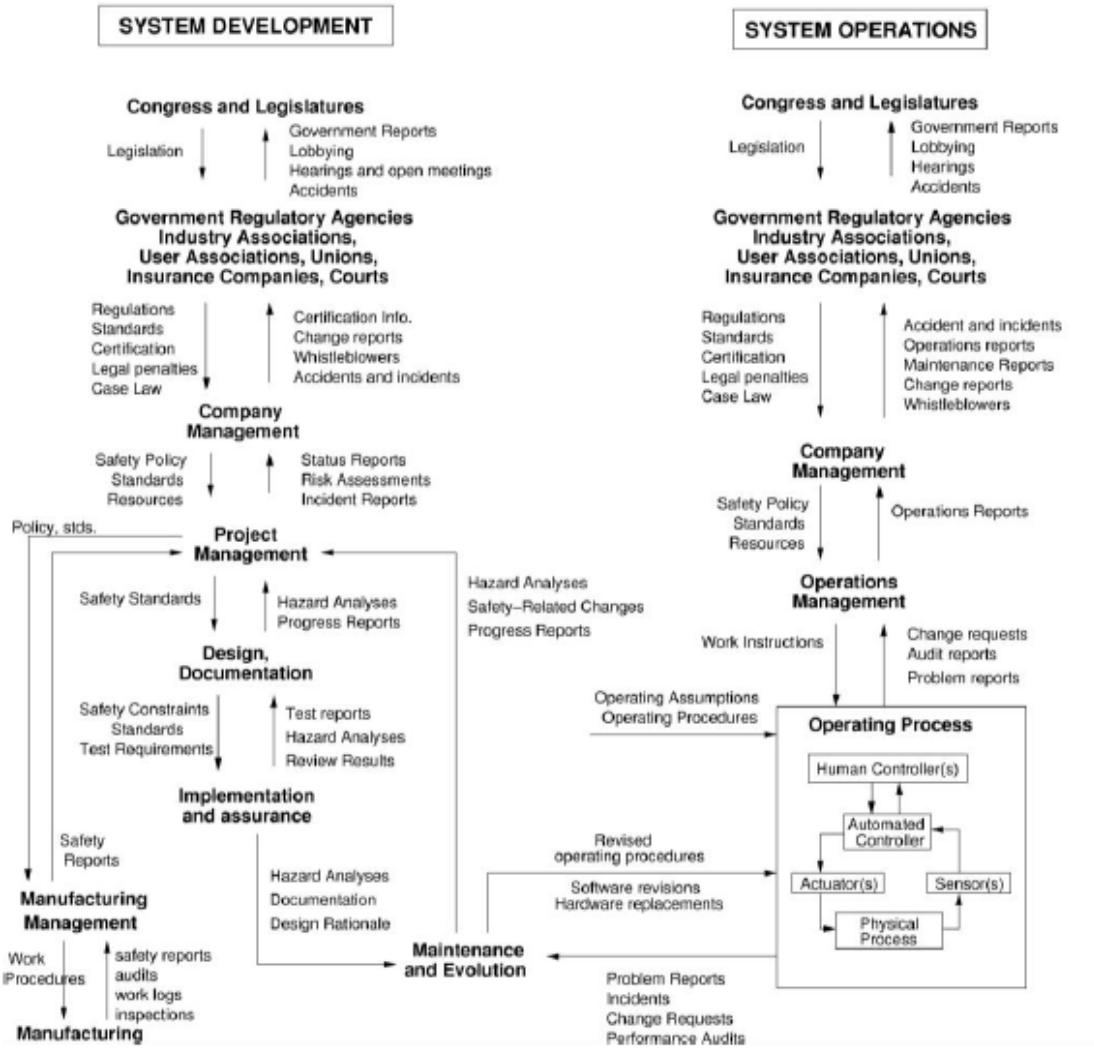


Figure 13 - An example safety control structure for a regulated industry

"Each component in the hierarchical safety control structure has responsibilities for enforcing safety constraints appropriate for that component, and together these responsibilities should result in enforcement of the overall system safety constraint. Part of defining the safety control structure is a specification of the expectations, responsibilities, authority, and accountability with respect to enforcing safety constraints of every component at every level. These responsibilities, authority, etc. taken together must enforce the system safety

constraints in the physical design, operations, management, and the social interactions and culture." [36]

As discussed in Chapter 7, the safety control structure model of the enterprise is only one of the design views of the enterprise. It is related to the other design views, as described in Section 7.3.5, but is useful in its support for performing the STPA analysis.

As described in Figure 12 above, the safety control structure can be used to help identify potential causes of unsafe control actions. To be more specific on the potential causes, it is useful to distinguish between human and technology based controllers and controlled processes. Figure 14 shows a safety control structure that incorporates both human and technology based controllers. The combinations of situations that can be analyzed are as follows:

- Human controller controlling humans,
- Human controller controlling technology, and
- Technology controller controlling technology.

In each case there are potential causes of unsafe control actions due to either the controller or the interface between the controller and the controlled process. Figure 15 through Figure 21 show the potential causes of unsafe control actions (UCAs) for each of the above situations. The list of potential causes of unsafe control actions from these figures can be used as a checklist in any specific analysis to aid in the identification of unsafe control actions.

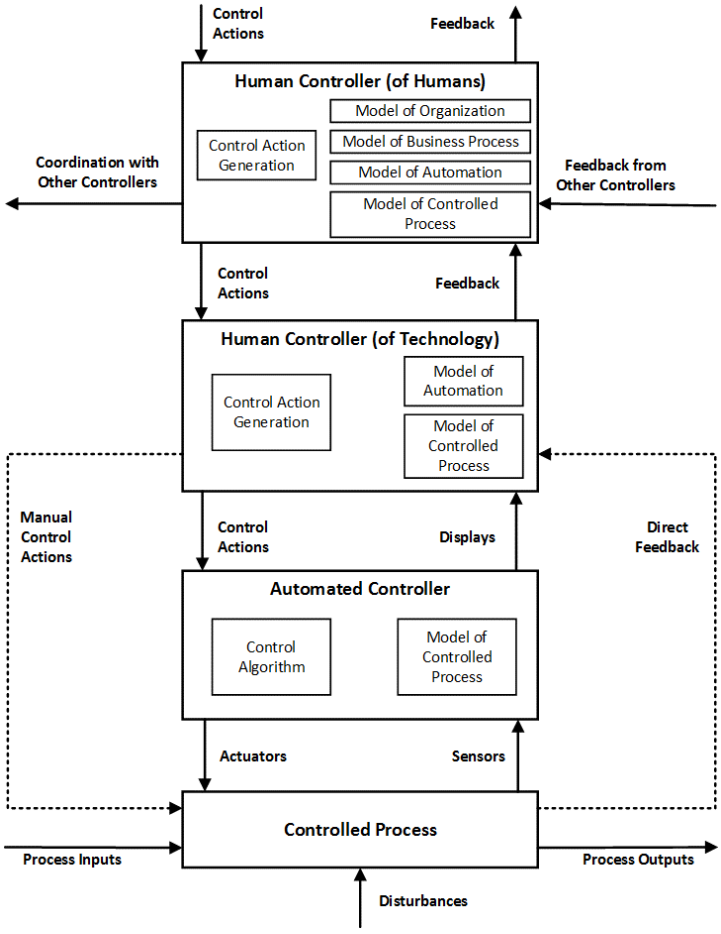


Figure 14 - Safety Control Structure Model - Human & Technology Controllers

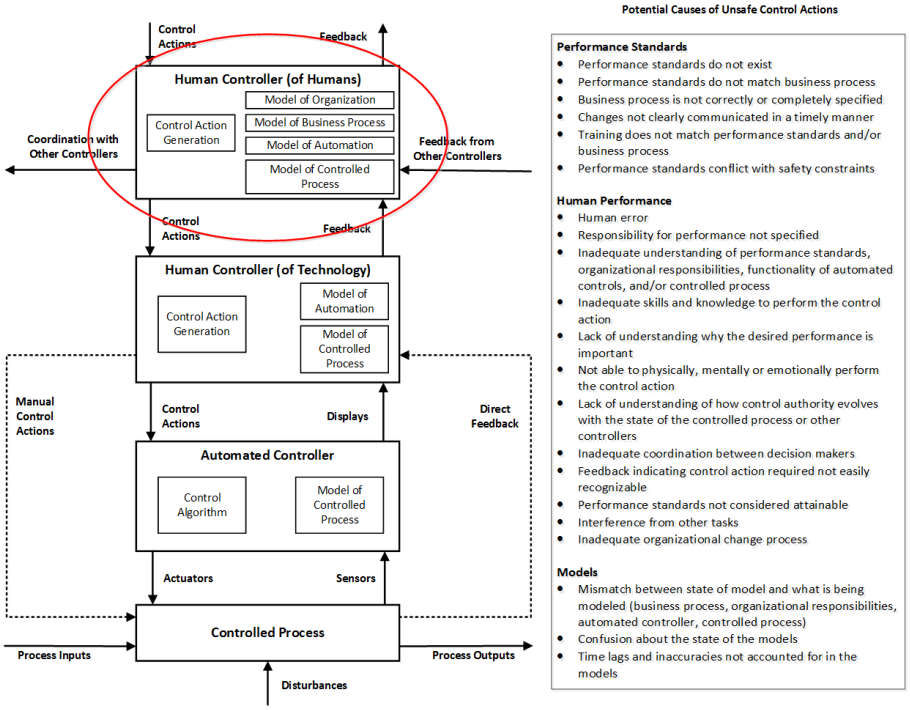


Figure 15 - Causes of UCAs - Controller of Humans

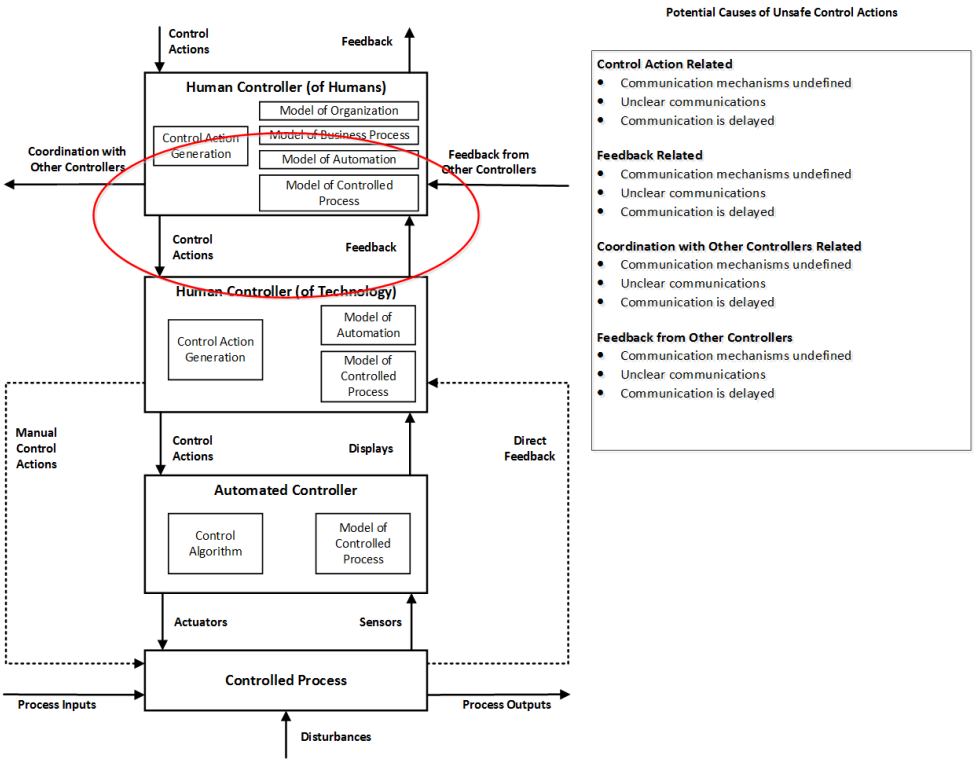


Figure 16 - Causes of UCAs - Human to Human Interface

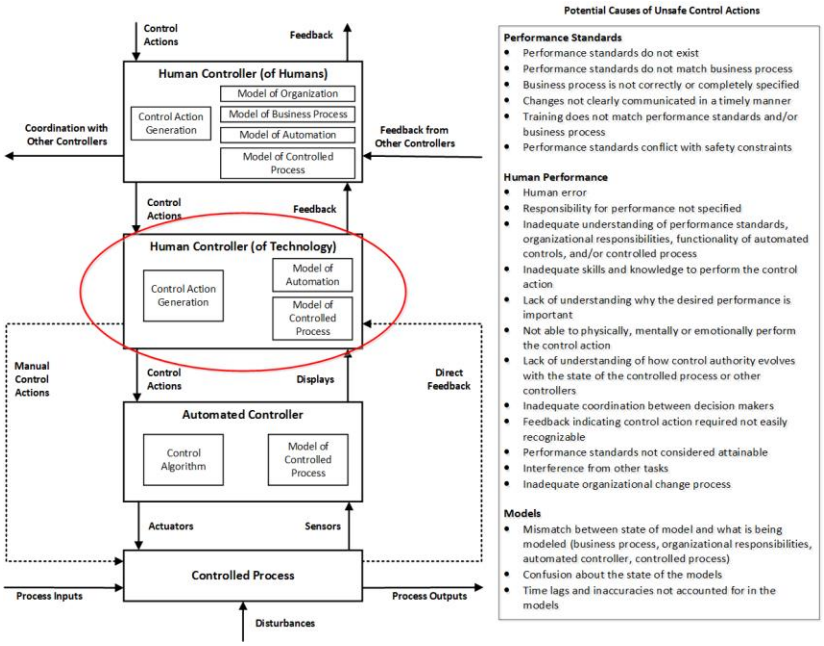


Figure 17 - Causes of UCAs - Human Controller of Technology

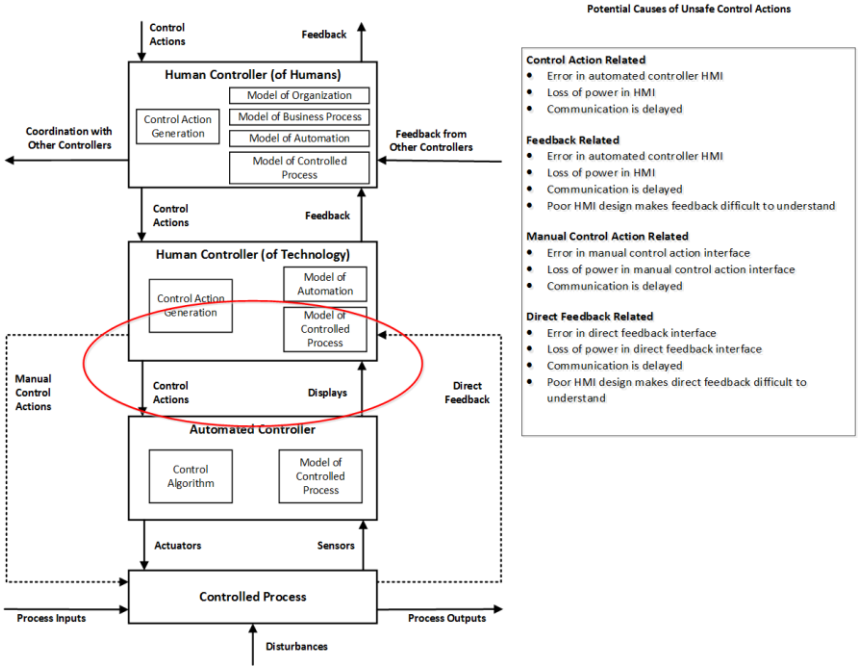


Figure 18 - Causes of UCAs - Human to Technology Interface

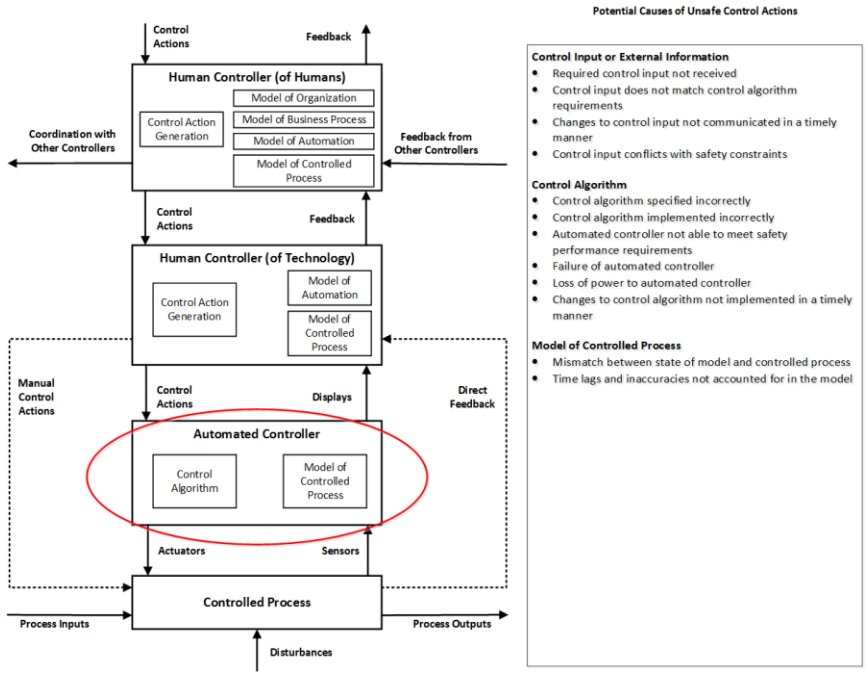


Figure 19 - Causes of UCAs - Technology Controller

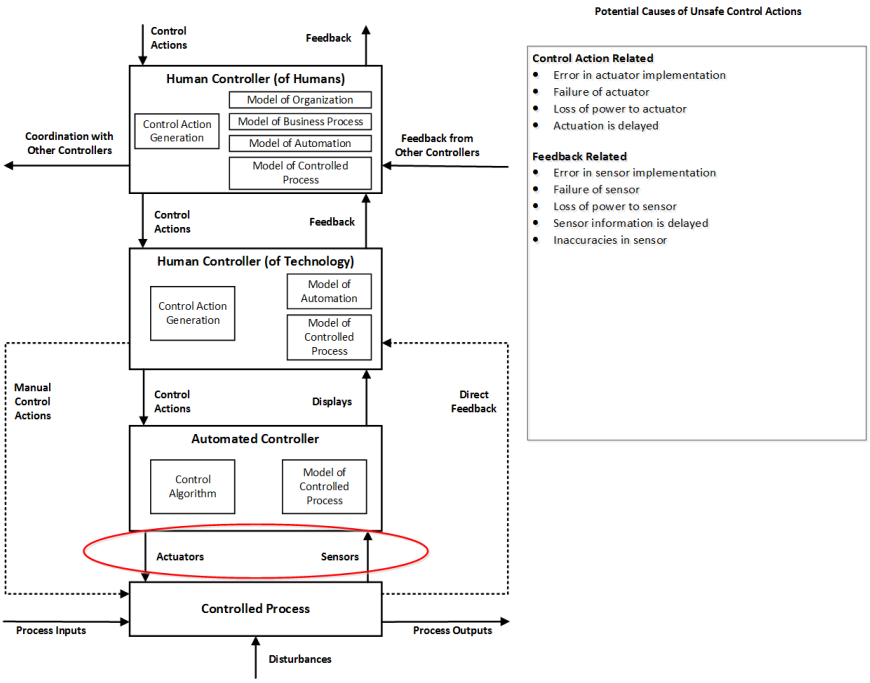


Figure 20 - Causes of UCAs - Technology to Technology Interface

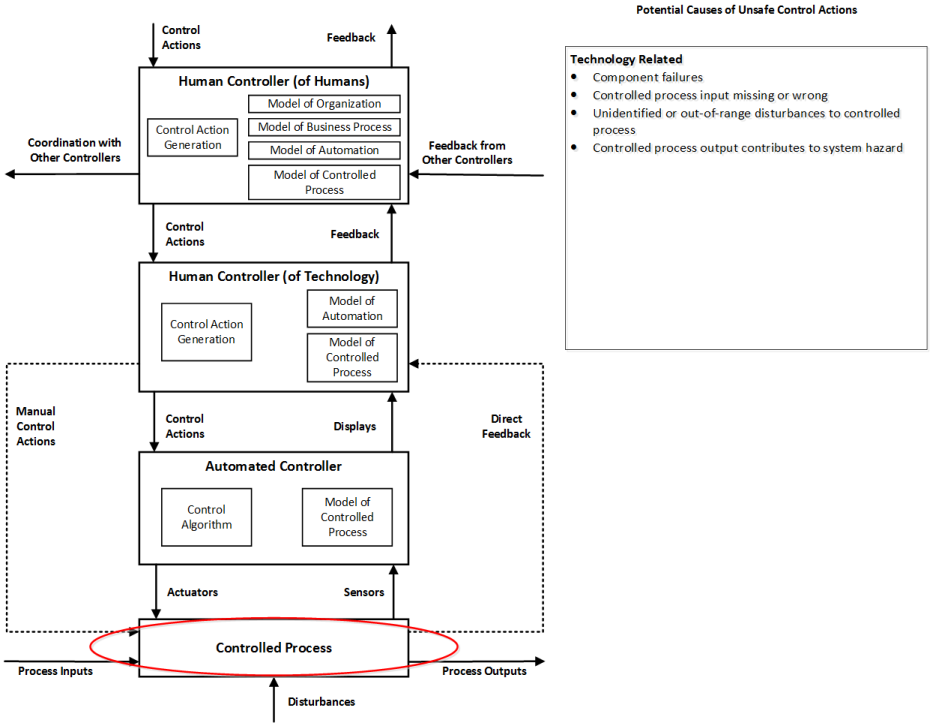


Figure 21 - Causes of UCAs - Controlled Process

In her work, Stringfellow [37], uses the safety control structure to develop factors that can cause unsafe control actions from an organizational perspective and from an individual perspective. Figure 22 shows the organizational factors and Figure 23 shows the individual factors.

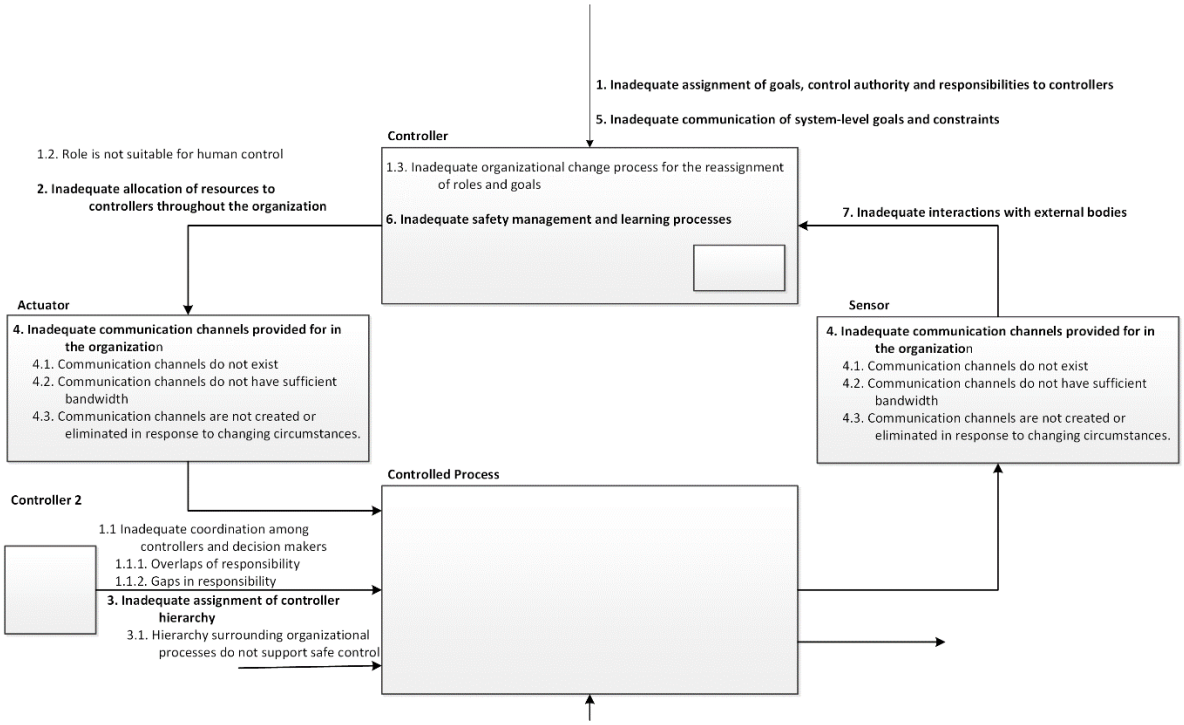


Figure 22 - Stringfellow Organizational Error Taxonomy

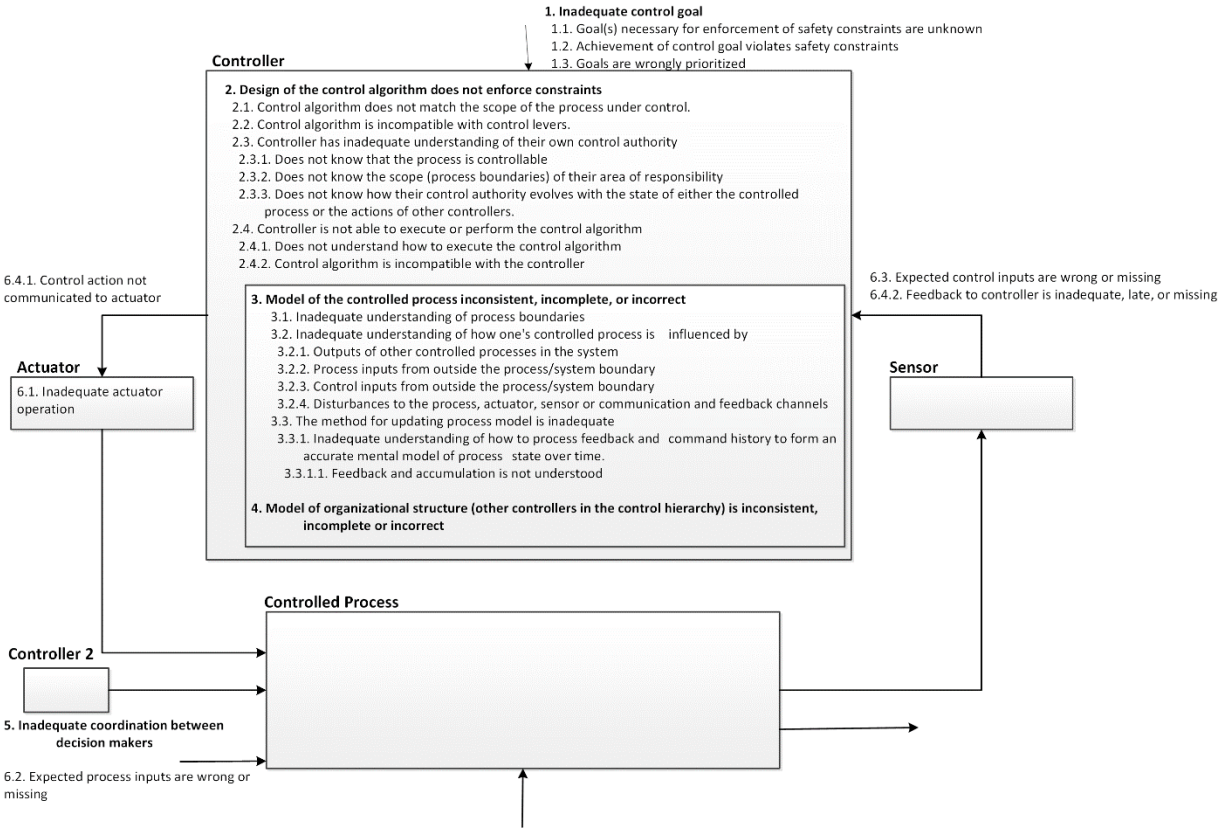


Figure 23 - Stringfellow Individual Error Taxonomy

In their work, Rummler and Brache describe one view of process improvement in terms of the human performance system [38]. Figure 24 shows their model of the human performance system and lists some of the factors that influence the successful operation of the human performance system. Given that the human performance system model is similar to the safety control structure model, these factors easily map to factors that can lead to unsafe control actions.

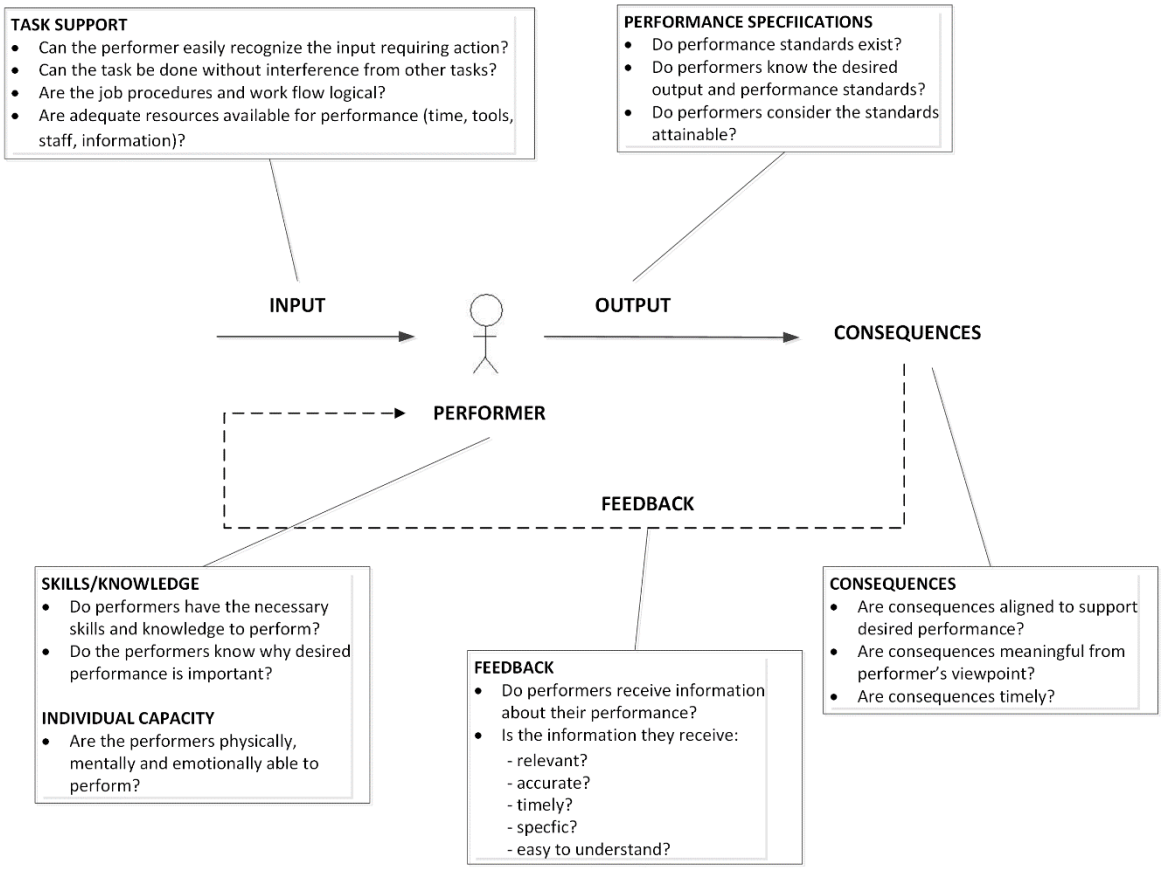


Figure 24 - Rummler-Brache Human Performance System [38]

The US Nuclear Regulatory Commission produced [4] to help improve regulatory review of complex systems. The document includes lists of potential causes of hazards and corresponding conditions that reduce the hazard space. The following areas were addressed by the document:

- Overall hazard analysis
- Organizational processes
- Technical processes
    - System concept
    - Requirements
    - Architecture
    - Hardware
    - Software design
    - Software implementation

7 MODEL OF AN ENTERPRISE

The design of any system results in a definition of the architecture, components, interfaces, and other characteristics of the system. This chapter defines an enterprise modeling framework that utilizes a number of modelling constructs to provide useful views of the design of the enterprise at the different levels of detail necessary to achieve a safety objective.

The enterprise model describes how people (with specific competencies within an organizational structure) perform necessary activities (both operational and decision making activities as defined by business processes) to design, construct, operate, maintain and decommission a potentially hazardous technology for which the enterprise is responsible. The focus on the design of the business processes, organizational structure, governance structure and the technology itself is to achieve a safety goal.

The Safety Enterprise Engineering process, as described in Chapter 5, will result in the definition of an enterprise design including the technology, organizational design, governance structure and business process design that is intended to achieve the enterprise's safety goals. The governance structure is represented in a "safety control structure view", which supports a technique of hazard analysis called Systems Theoretic Process Analysis (STPA) as described in Chapter 6.

Figure 25 shows the core business processes and their context for any enterprise that is responsible for a hazardous technology. In the center of the figure is the hazardous technology. Around the technology are the business processes required to design, operate, maintain and modify the technology. Surrounding the core business processes and the technology are the business processes that monitor the performance of the technology and the core business processes and then takes action to improve them if they are not performing consistent with expectations (Enterprise Performance Monitoring and Continuous Improvement). The environment within which the enterprise operates is partitioned into its technological aspects, sociological aspects and natural aspects.

Figure 26 shows the various elements that make up the enterprise model. Each of these elements is described in more detail in section 7.2. Business processes are made up of enterprise activities. Each activity is the responsibility of an organizational unit within which individuals are assigned organizational roles.

Each individual has a profile of skills. Each enterprise activity provides a defined capability.

Section 7.1 describes the overall enterprise modelling framework including the relevant enterprise lifecycle phases, design views, and representations at different levels of abstraction. Section 7.2 describes each of the modelling constructs used to model the enterprise. Section 7.3 describes a number of design views based on the modelling constructs that are useful in the course of engineering a safe enterprise.

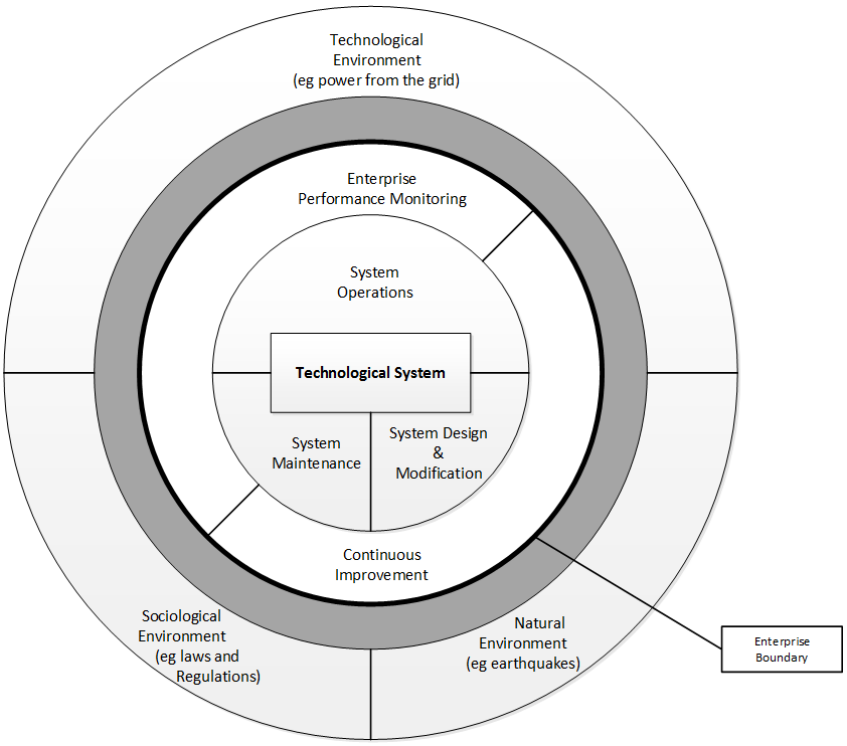


Figure 25 - Core Business Processes for an Enterprise and Their Context

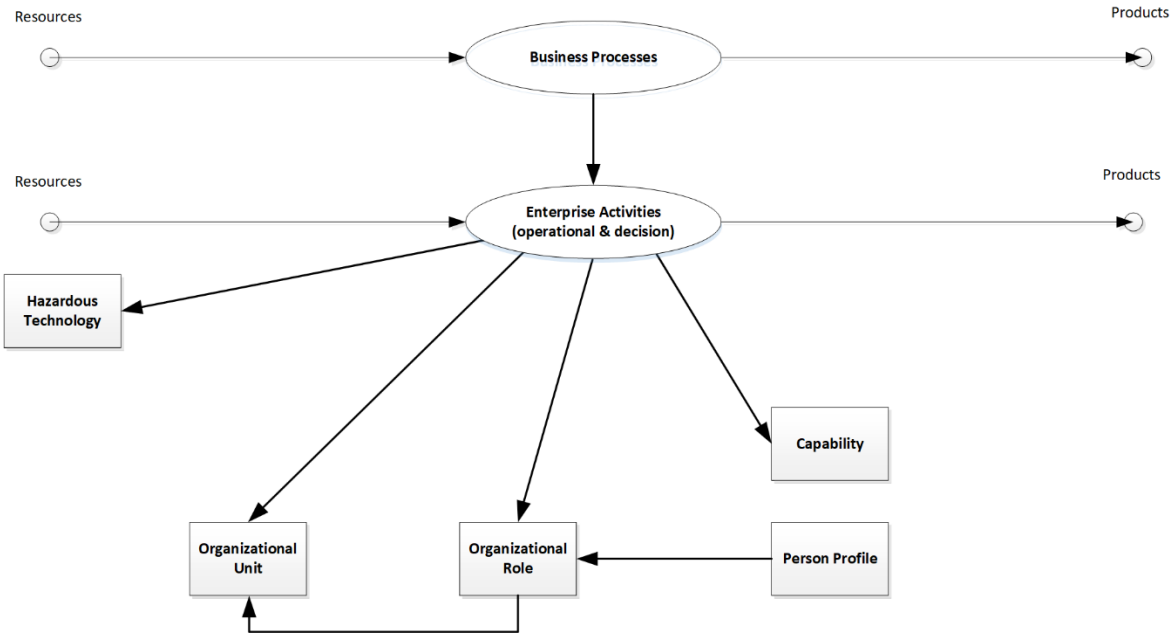


Figure 26 - Elements of the Enterprise Model

7.1 Enterprise Modeling Framework

Figure 27 shows some of the standards that ISO has produced that define enterprise modeling framework concepts. The thesis uses the concepts in these standards, but focuses on achieving a safety objective.

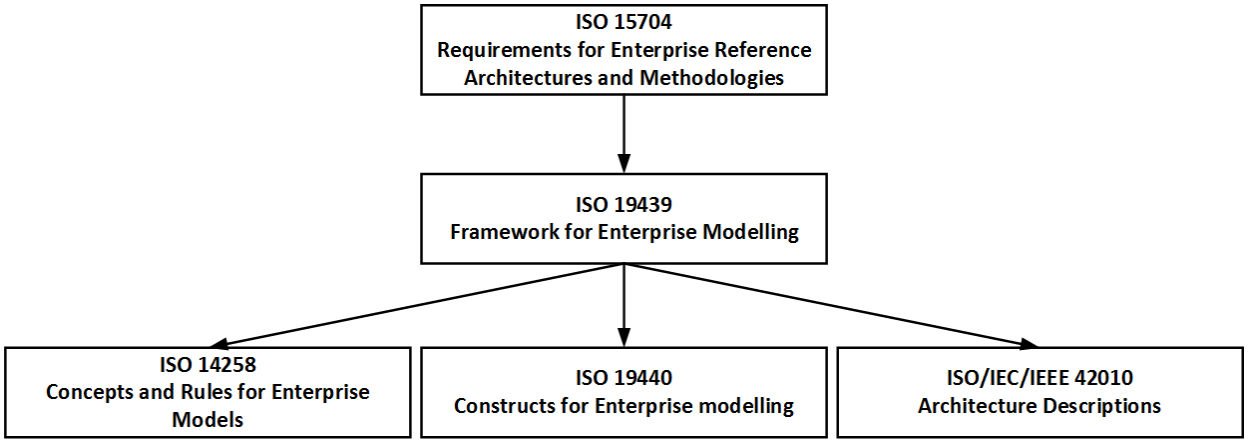


Figure 27 - ISO Enterprise Modeling Related Standards [25], [26], [27], [28], [29]

A modelling framework defines both the constructs used to define an enterprise but also separates descriptions of the enterprise by useful distinctions. Three fundamental distinctions will be used for the enterprise modeling framework. The three distinctions are:

1) Lifecycle phase: Design & Construction, Operations & Maintenance, and Decommissioning
2) Level of Specificity: Generic, Partial, Specific models
3) Design Views: Technology View, Organizational View, Process View, and Safety Control Structure View

Figure 28 shows the generic framework defined by ISO 19439 [26]. Each of the three distinctions mentioned above are reflected in the three axes of the figure. Figure 29 shows the specific framework that will be adopted by this thesis based on the generic framework in ISO 19439 [26], but focused on meeting the needs of the nuclear power industry domain.

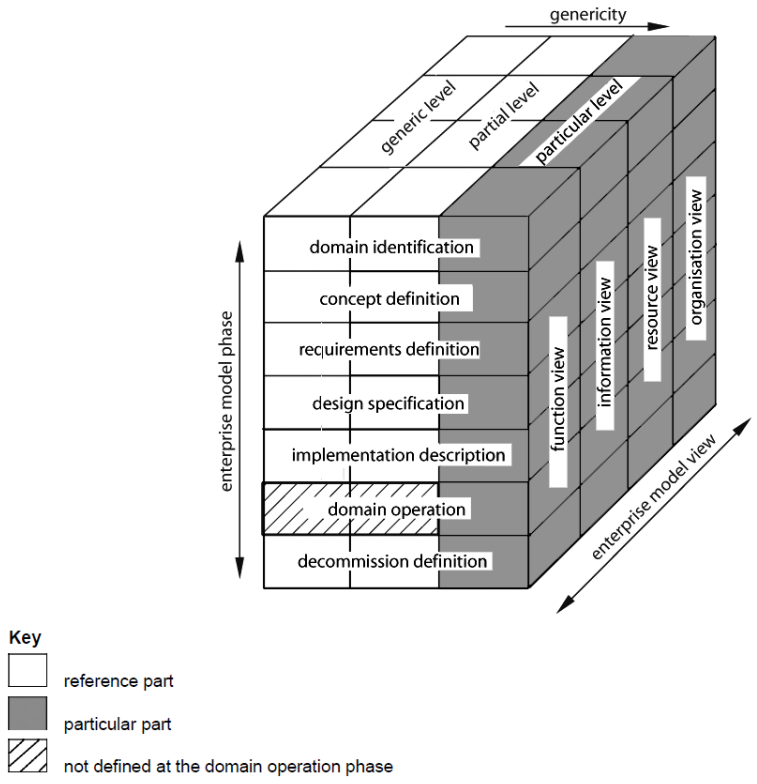


Figure 28 - ISO 19439 Framework for Enterprise Modeling [26]

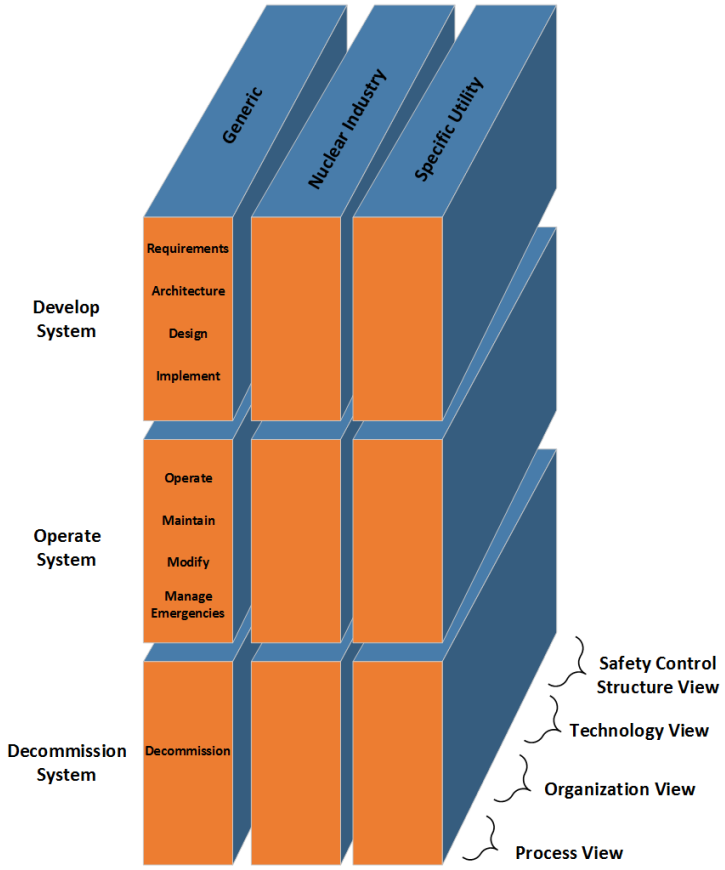


Figure 29 - Enterprise Modeling Framework for Nuclear Industry

7.1.1 Lifecycle Phases

There are many possible phases of the lifecycle of an enterprise. From a safety perspective, three distinct phases are relevant: Design and Construction, Operations and Maintenance, and Decommissioning.

During the design phase of the enterprise the focus is on designing the technology itself along with the business processes and organizational structures that will operate and maintain the technology. The safety goal is to identify hazards, and then incorporate into the design the elimination, control or mitigation of the causes of the hazards, and finally incorporating protection from degradation of safety over the life of the enterprise. During the implementation of the enterprise the focus is on assuring that each element of the design is implemented consistent

with its design specifications, and that the integrated set of elements satisfies the overall safety requirements.

During the operations and maintenance phase, the focus is on assuring that the technology is operated consistent with the safe operating envelope established during the design phase, and that the technology is maintained in a timely manner such that each element's performance is compliant with the safety requirements allocated to that element. Changes made to the design during the operations and maintenance phase must ensure that safety requirements are still satisfied after the change, and that no new hazards have been introduced that are not addressed by the design.

During decommissioning, the focus is on assuring that hazards are identified and adequately eliminated, controlled or mitigated by the decommissioning process for each state that the technology goes through until fully decommissioned.

During all phases, it is critical to monitor performance of the enterprise (people, processes and technology) to ensure that its actual performance is consistent with the design's assumed performance and that effective corrective actions are taken if any inconsistencies are detected.

Each of the lifecycle phases uses models necessary to facilitate achievement of the safety objective for the phase. Each of the models can be defined at different levels of specificity (generic, partial or specific). The following sections define the models necessary for each phase.

7.1.1.1 Design and Construction Phase

During this phase, the safety objective is to design and construct a technology (for example a nuclear power plant) that can be operated safely. Achieving this safety objective will be a function of the design process used, the capabilities of the people performing the design process and ultimately a function of the design and implementation of the technology.

Hence the business processes, organizations and governance structure must also be engineered consistent with the safety objective of the enterprise. This results in models of the technology, business processes, and organization required to represent the products of this phase to demonstrate achievement of the safety

objective. As noted earlier, a safety control structure representation is also required to document the governance structure and to facilitate effective hazard analysis.

Monitoring the performance of the business processes and organizations is critical to provide assurance that the safety objective for this phase is achieved and to provide for continuous improvement over time.

7.1.1.2 Operations and Maintenance Phase

During the operations and maintenance phase, the safety objective is to operate the technology consistent with its safe operating envelope, and to maintain the technology such that it continues to satisfy its safety requirements over its operating life. Achieving this safety objective will be a function of the operations and maintenance processes, and the capabilities of the people performing the operations and maintenance processes.

Hence models of the business processes and organization are required to demonstrate achievement of the safety objective. As noted earlier, a safety control structure representation is also required to facilitate effective hazard analysis.

Monitoring the performance of the business processes, organizations and the technology itself is critical to provide assurance that the safety objective for this phase is achieved and to provide for continuous improvement over time.

Clearly having a well documented safe operating envelope and safety requirements for the technology are pre-requisites to achieving the safety objectives for this phase.

7.1.1.3 Decommissioning Phase

As a technology is decommissioned it is will go through various intermediate states between operating and fully decommissioned. Hazard analysis for these intermediate states needs to be performed to establish means to eliminate, control or mitigate hazards. The design of these intermediate states, the business

processes used to move from state to state and the capabilities of the people performing the business processes needs to be defined to assure that the safety objective is achieved for this phase.

7.1.2 Level of Specificity

The enterprise modeling framework in ISO 19439 [26] defines three levels of specificity for an enterprise model: generic, partial and specific.

The generic level of specificity in this thesis defines concepts necessary to achieve safety that are applicable to any enterprise. "At the generic level, a reference catalogue of generic modelling language constructs for expressing descriptions of the entity to be modelled are defined for each of the enterprise model phases. These modelling language constructs are then be used to create models at each of the partial and particular levels." [26]

The partial level of specificity describes concepts necessary to achieve safety within a specific domain but in a manner that makes the model applicable to a number of specific implementations. "At the partial level, sets of partial models are described for each of the enterprise model phases, which express typical functionalities, information, resources and organization belonging to particular industry segments (in this thesis the nuclear power industry is used). These models can generate models at the particular level by further instantiation and specialization." [26]

The specific level of specificity is a representation of a specific implementation of the partial model necessary to achieve safety for a specific enterprise. The implementation within a particular nuclear power utility is an example of the specific level.

The work in this thesis focuses on the nuclear power industry and hence presents a partial enterprise model for a nuclear power utility.

7.1.2.1 Generic Level

The generic level consists of a collection of constructs that can be used to build a partial model within a particular domain. The set of constructs defined in this thesis were chosen and defined to be able to support the implementation of a safe enterprise. A key aspect of this is the ability to present design views of the technology, people and processes that are relevant to achieving the safety goal during all lifecycle phases of the enterprise. The ability to project these elements into a safety control structure view of the enterprise is key so as to be able to support an STPA based hazard analysis and then map the results of the hazard analysis back to the design of the technology, organizations and business processes.

Section 5.2 defines the set of enterprise modelling constructs and Section 5.3 defines the design views that utilize the constructs.

7.1.2.2 Partial Level

The partial level consists of a partial model that utilizes the constructs of the generic level to create a re-usable reference model for a particular industry segment. This thesis defines a partial model for a utility in the nuclear power industry. The partial model needs to be instantiated to create a model of a specific nuclear power utility.

Chapter 7.4 defines a partial model for a nuclear power utility based on nuclear power industry best practice documents.

7.1.2.3 Specific Level

"The particular level shall be concerned solely with one particular enterprise domain. It shall embody all necessary knowledge of that enterprise in a way that can be used directly for the identification, specification, implementation, operation and later decommissioning of its enterprise operation." [26]

The specific level in this thesis would correspond to the actual organization, business processes and plant design used by a nuclear power utility such as TEPCO in Japan that was responsible for the Fukushima nuclear power plant.

Note, that the analysis in the example is based on the partial model in section 7.4 as applied to a CANDU based utility since insufficient information is available about the specific organizational, business process model and plant design at Fukushima, and the fact that the author has 30 years experience and hence is familiar with a CANDU based utility.

7.1.3 Design Views

Clearly the design, construction, operation, maintenance and decommissioning of the technology that can present a hazard is a fundamental focus of the engineering efforts.

The technology view of the design captures the design of the specific technology relevant to achieving the safety goal.

As noted earlier, hazards can also come about due to the performance of the processes used to design, construct, operate, maintain and decommission the technology. The process view of the enterprise captures the key aspects of the processes prerequisite to achieving safety.

The performance of the people in organizations that execute the processes can also result in hazards. The organizational view of the enterprise captures key aspects of the people and their organizations that are prerequisite to achieving safety.

Effective hazard analysis is one prerequisite to achieving safety. As discussed earlier, traditional methods of hazard analysis are not effective for large complex systems such as are reflected by enterprises. One method of hazard analysis that is effective for these complex systems is STPA (Systems Theoretic Process Analysis) [36]. STPA is based on analysis of a safety control structure model of the enterprise. Hence a Safety Control Structure view of the enterprise is another necessary view to support effective hazard analysis.

Section 7.3 defines these various views using the modelling constructs defined in section 7.2 along with the relationships between the views.

7.2 Model Constructs

The generic level of the enterprise modelling framework defines modelling constructs that can be used to represent various views of the design of the enterprise. Appendix 2 defines each of these modelling constructs. For each modelling construct, its purpose, key attributes and relationships to other constructs is defined. The following modelling constructs are defined:

- Organizational Unit
- Organizational Role
- Person Profile
- Capability
- Resource
- Enterprise Object
- Decision Centre
- Business Process
- Enterprise Activity
- Technology Element

7.3 Design Views

The design of the enterprise can be represented by different views that focus on specific aspects of the unified enterprise model that are prerequisite to achieving the safety objective. As discussed, four useful views are:

- the technology view,
- the business process view,
- the organizational view and
- the safety control structure view.

“Views contain a subset of facts present in the integrated model in order to concentrate on relevant questions that the respective stakeholders may wish to consider using enterprise modelling. Different views may be made available, highlighting certain aspects of the model and hiding others. The concept of view is applicable to models of all entity types across their entire life cycle.” [25]

The following sections define what information is presented in each view.

7.3.1 Technology View

The technology view provides a representation of the technology[6] allowing it to be constructed, operated, maintained, modified and decommissioned.

The technology can be viewed as a system. System engineering standards [23] define a system as a collection of interacting elements organized to achieve one or more stated purposes. In the context of a stepwise refinement approach to design, an element of a system can be considered a system (sub-system) and be further decomposed into interacting elements.

Hence the technology can be represented at various levels of abstraction. For example, a nuclear power plant could be represented by technology elements representing the major systems within the plant, see Figure 30 and Figure 36. At an intermediate level of abstraction, each of the major systems can be decomposed into their constituent technology elements. Figure 31 and Figure 37 show the decomposition of the control system technology element. At the lowest level of abstraction a particular control system can be shown in terms of the specific hardware and software technology elements used to implement the control system.

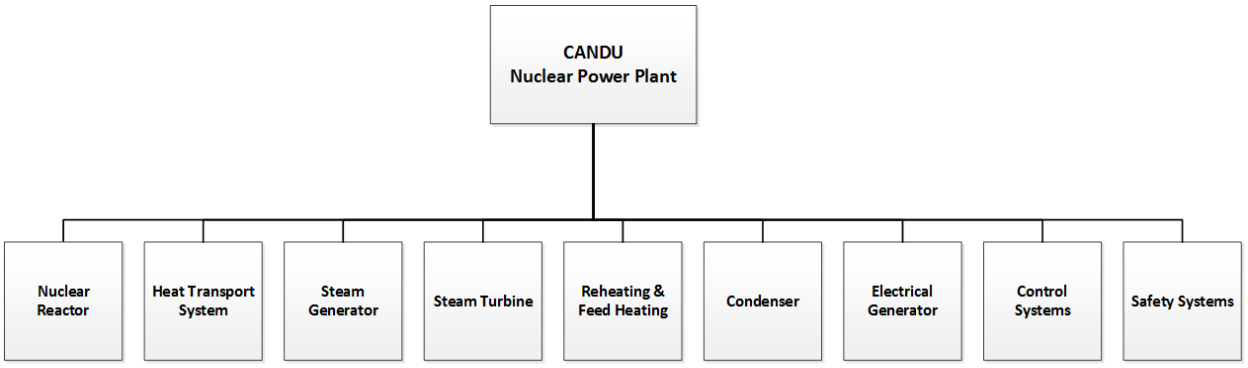


Figure 30 - Major Systems in a CANDU Nuclear Power Plant [39]

[6] The technology referred to here is a technology that the enterprise is responsible for and that can potentially enter a hazardous state and hence has raised the safety concern.

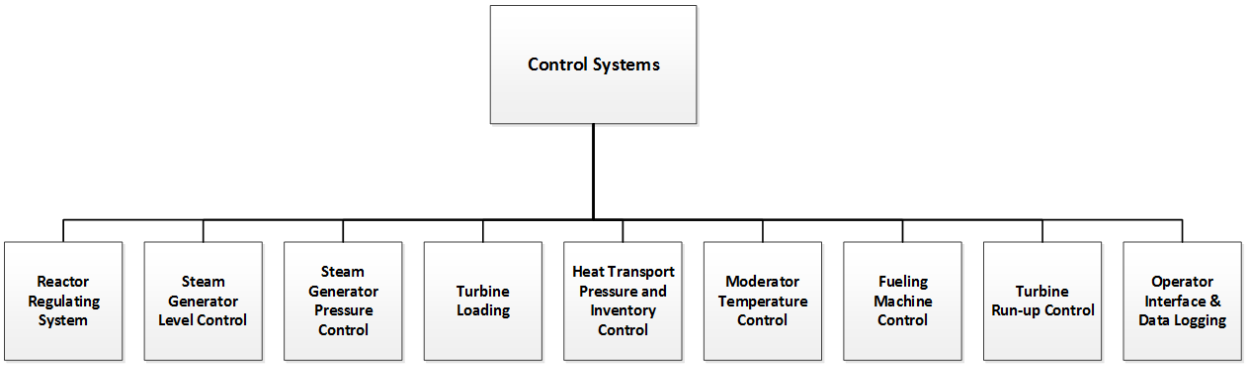


Figure 31 - Control Systems in a CANDU Nuclear Power Plant [39]

7.3.2 Business Process View

Business processes define the activities that are undertaken to design, construct, operate, maintain, modify and decommission the technology. The business process view enables the representation and modification of the processes of the enterprise, their functionalities, behaviours, inputs and outputs [26].

Business processes can be modelled at different levels of abstraction. Figure 32 and Figure 38 show the business processes used to operate a nuclear power plant, at a high level of abstraction. Each business process can be modelled using the Business Process construct. At an intermediate level of abstraction, each of the processes can be decomposed into their sub-processes as shown in Figure 33 and Figure 39, where each sub-process can be modeled using the Business Process construct. Finally, at the detailed level of abstraction, the specific practices to be used for each sub-process can be defined and modeled using the Enterprise Activity construct. Industry documents such as [40], which provides guidance for the Equipment Reliability sub-process, provide guidance for each sub-process.

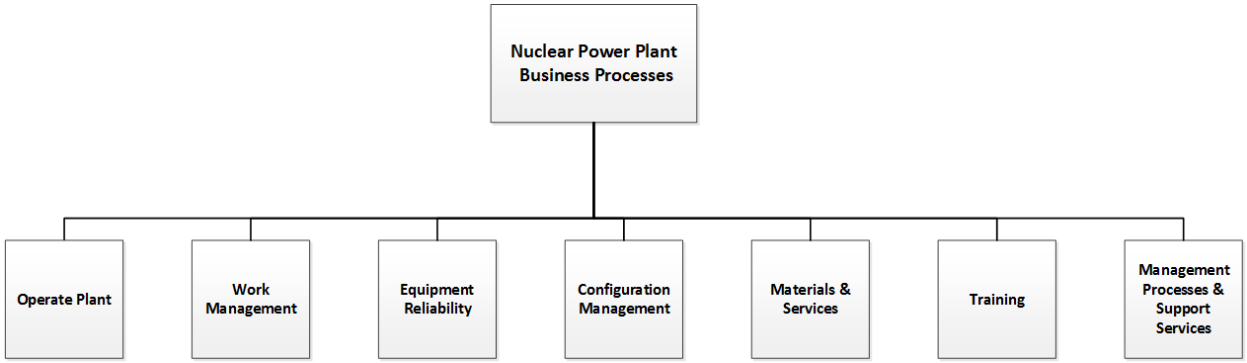


Figure 32 - Nuclear Power Plant Processes [41]

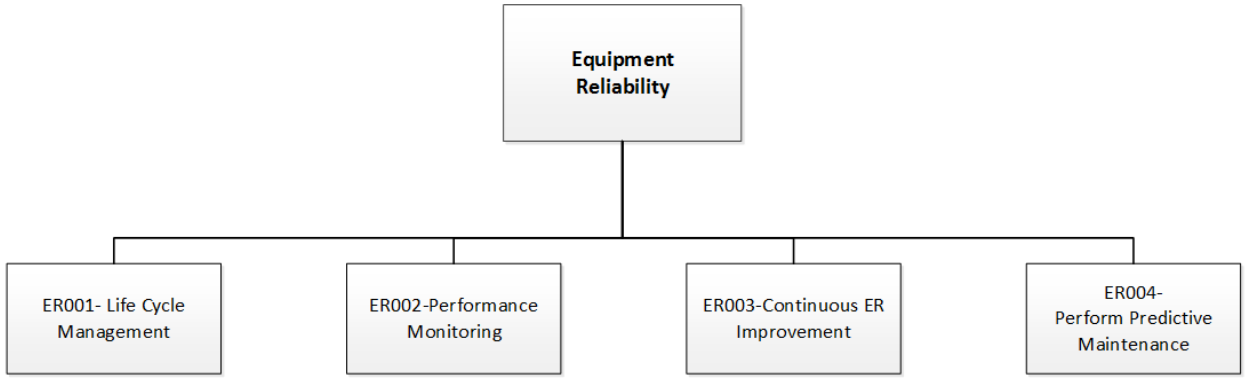


Figure 33 – Sub-processes for Equipment Reliability Process [41]

Enterprise Activities can either be operational activities or management / decisional activities. Operational activities are focused on transforming inputs into outputs along the value stream of the enterprise. Management / decisional activities make decisions about the resourcing and scheduling of the operational activities. The governance structure of the enterprise is presented using the concept of Decision Centres which is an allocation of sets of management / decision making activities to specific organizational units.

7.3.3 Organizational View

The organizational view defines the organizational units, the organizational roles allocated to each unit and the skills required of people in those roles necessary to competently carry out the responsibilities of their role, and the decision centres that represent the decision making or governance roles within the enterprise.

"The organization view shall describe the responsibilities and authorities within the enterprise domain. This view shall allow for the gathering and structuring of the different responsibilities (for processes, material, information, resource and control) in the enterprise, and include the mapping of those responsibilities onto the organizational entities and/or organizational groupings such as departments, divisions and Sections. The organization view shall also provide for representation of responsibilities for decisional activities into a decisional structure for the verification of consistency and completeness." [26]

7.3.4 Safety Control Structure View

"In systems theory, systems are viewed as hierarchical structures, where each level imposes constraints on the activity of the level beneath it- that is, constraints or lack of constraints at a higher level allow or control lower-level behavior.

Control processes operate between levels to control the processes at lower levels in the hierarchy. These control processes enforce the safety constraints for which the control process is responsible. Accidents occur when these processes provide inadequate control and the safety constraints are violated in the behavior of the lower-level components.

By describing accidents in terms of a hierarchy of control based on adaptive feedback mechanisms, adaptation plays a central role in the understanding and prevention of accidents." [2]

The safety control structure view is based on a feedback control system, as shown in Figure 34, as a standardized structure for creating a hierarchical model of the enterprise. Section 7.3.5 below shows the relationships between the safety control structure view and the other views of the enterprise.

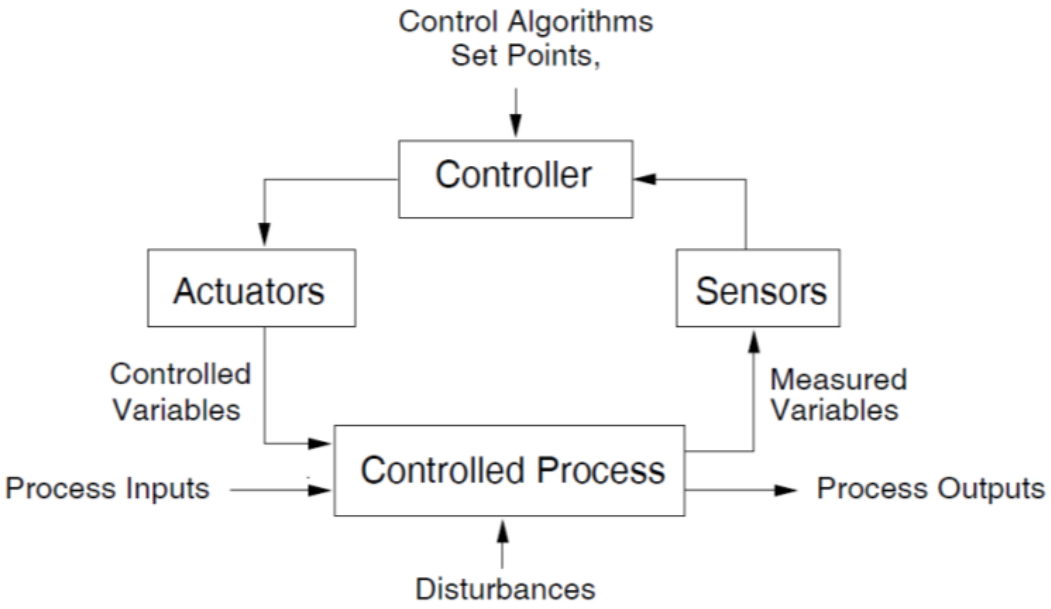


Figure 34 - Standard Feedback Control Loop

7.3.5 Relationships Between Views

The whole, integrated enterprise consists of all the elements reflected in the technology, process and organizational view. In order for the whole enterprise to be well integrated there are certain relationships that must be true between the elements in the various views. Figure 35 shows the various views discussed in the previous Sections and identifies the relationships A through F that must be true between the various views.

Hazard analysis based on the safety control structure will result in some recommendations for changes to the design based on analysis of the safety control structure. The relationships between the safety control structure view and the other views of the enterprise design must support mapping these changes from the safety control structure view to the other views so that the changes can result in changes to the design of the technology, business processes and/or organizational structure.

A: Organizational – Process View Relationships

A-1: There must be at least one Organizational Unit responsible for every Business Process and Enterprise activity.

A-2: People assigned an organizational role must have the knowledge and skills necessary to perform the Enterprise Activities assigned to that organizational role.

B: Organizational – Technology View Relationships

B-1: Every Technology Element must have an Organizational Unit responsible for the Business Process or Enterprise Activity associated with its design, its operations, its maintenance, its modification and its decommissioning.

C: Process – Technology View Relationships

C-1: Every Technology Element must have a Business Process or Enterprise Activity associated with its design, its operations, its maintenance, its modification and its decommissioning.

D, E and F: Organizational, Process and Technology – Safety Control Structure View Relationships

D-1: Every Decision Center must be mapped to a controller in the Safety Control Structure View (SCSV).

E-1: Every operational Business Process and Enterprise Activity must be mapped to a process being controlled in the SCSV.

F-1: Every Technology Element must be mapped to some element of the SCSV (controller, process being controlled, actuator or sensor).

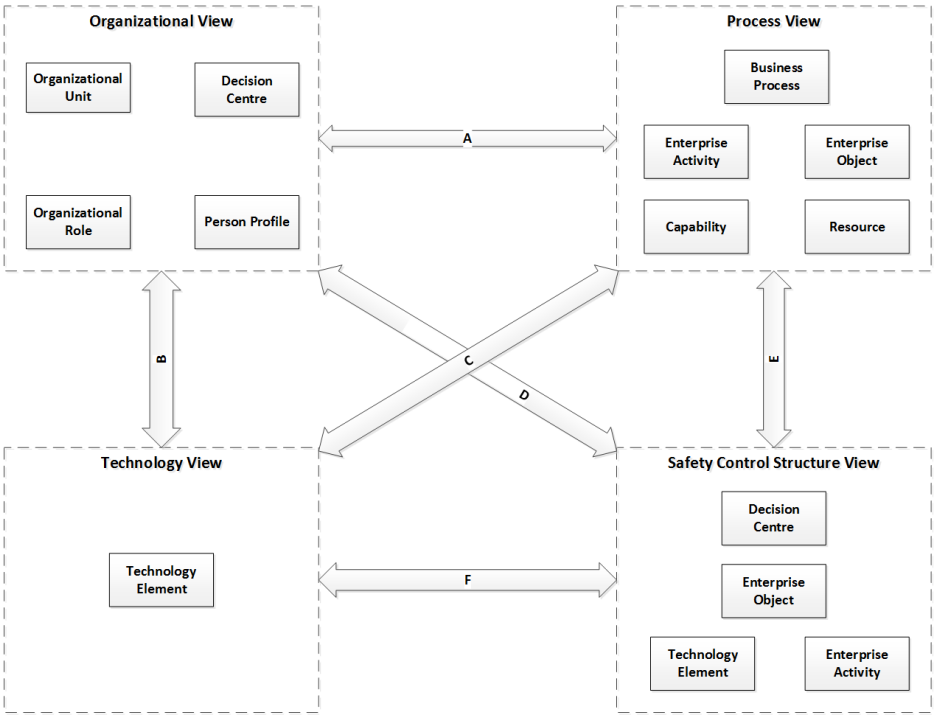


Figure 35 - Relationship Between the Views of the Enterprise

7.4 Nuclear Power Industry Partial Model

This section defines a partial model of a nuclear power utility using the generic modelling constructs defined in section 7.2. The design views defined in section 7.3 are used to present those relevant design views of the partial model.

This partial model of a nuclear power utility is used to illustrate the use of the modeling constructs and design views defined earlier, and is used as input to the example in Chapter 11.

Much of the content of the partial view is based on references [39], [41] and [42].

7.4.1 Technology View

Figure 36 shows a typical architecture of a CANDU nuclear plant showing the major systems within the plant. Figure 30 shows the list of major systems in the plant. Each of these major systems can be decomposed into the systems that make

up that major system. Figure 31 and Figure 37 show the decomposition of the control systems in the plant.

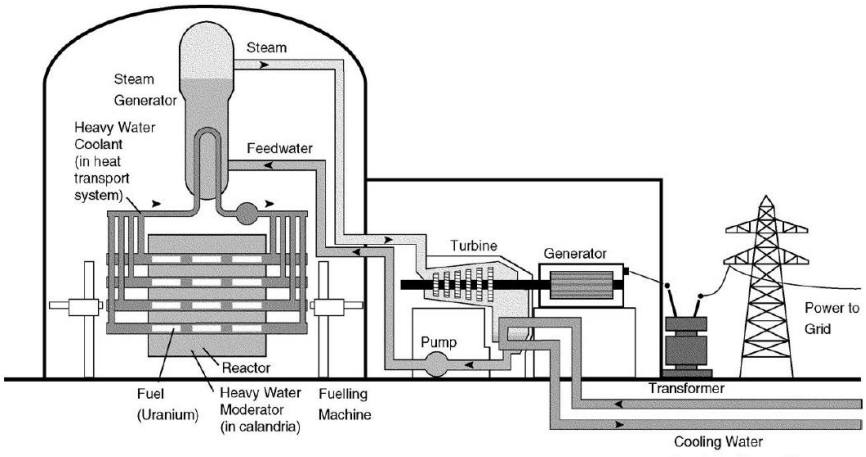


Figure 36 - Typical Architecture of a CANDU Nuclear Plant [39]

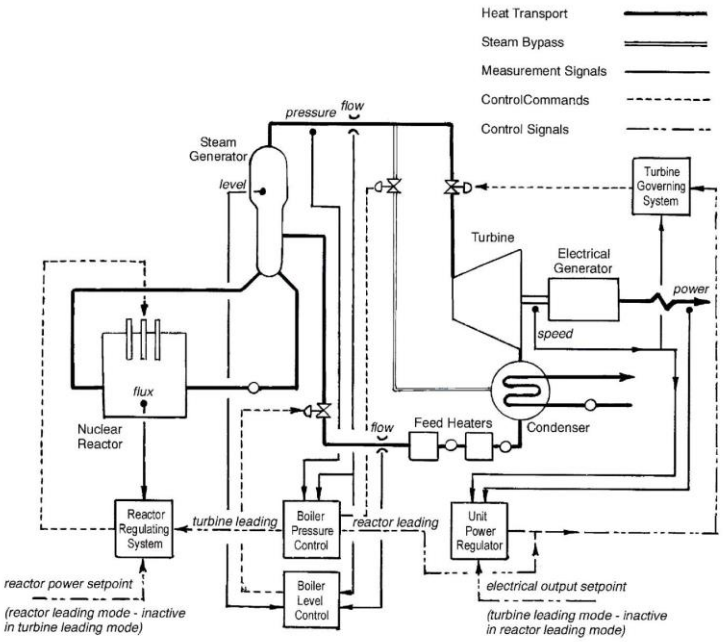


Figure 37 - Basic CANDU Plant Control System [39]

7.4.2 Business Process View

Figure 38 shows a high level view of the business processes required to operate a nuclear power plant based on [41]. Figure 39 shows the sub-processes that make up each of the business processes.

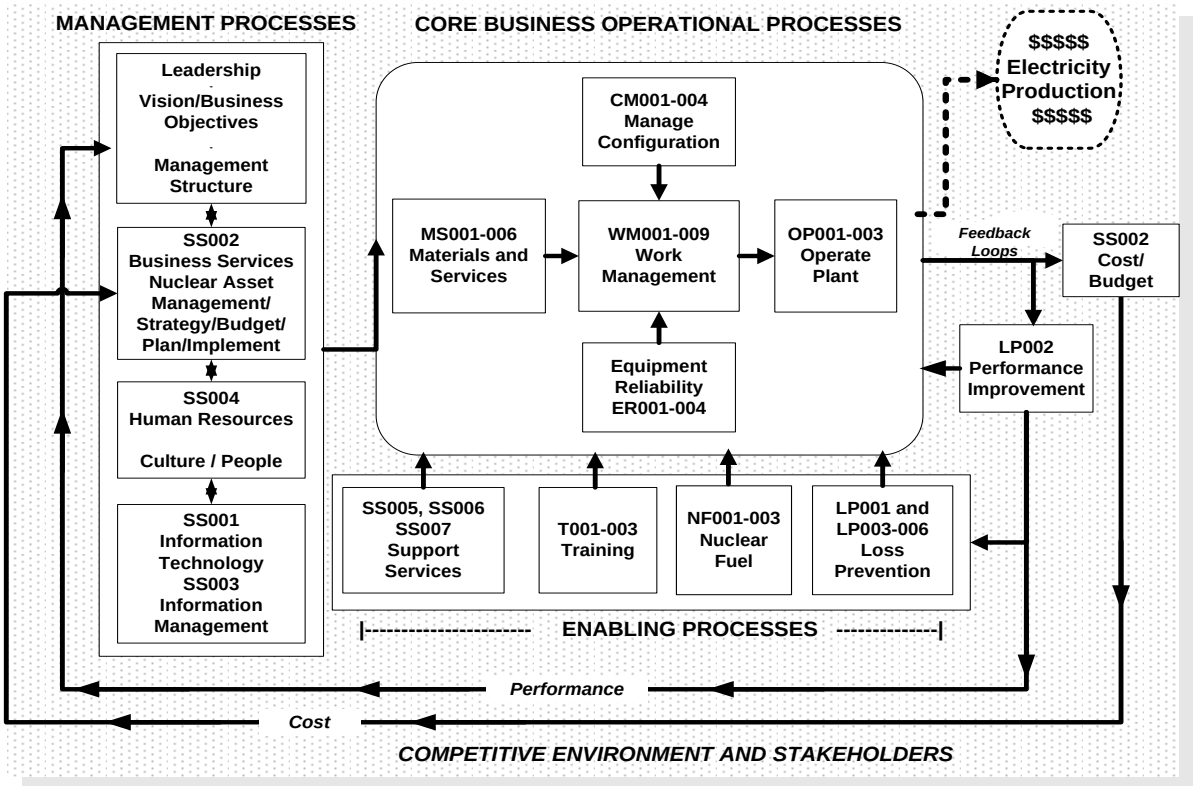


Figure 38 - Standard Nuclear Performance Model – Executive View [41]

OPERATE PLANT	WORK MANAGEMENT	EQUIPMENT RELIABILITY	CONFIGURATION MANAGEMENT	MATERIALS & SERVICES	TRAINING	LOSS PREVENTION	MANAGEMENT PROCESSES AND SUPPORT SERVICES
• OP001-Operate & Monitor Structures, Systems and Components • OP002-Monitor & Control Effluents • OP003-Monitor & Control Plant Chemistry	• WM001-Perform Planning • WM002-Perform Scheduling • WM003-Perform Preventive Maintenance • WM004-Perform Corrective Maintenance • WM005-Maintain Non-Plant Equipment • WM006-Perform Plant Improvement Maintenance • WM007-Monitor & Control Radiation Exposure • WM008-Monitor & Control Contamination • WM009-Perform Minor Maintenance/ Fix-It-Now Maintenance	• ER001-Life Cycle Management • ER002-Performance Monitoring • ER003-Continuous ER Improvement • ER004-Perform Predictive Maintenance	• CM001-Evaluate Problem or Desired Change • CM002-Change Design Requirements • CM003-Change Physical Configuration • CM004-Change Facility Configuration Information **NUCLEAR FUEL** • NF001-Provide Fuel Management Services • NF002-Provide & Transport Fuel • NF003-Provide Handling, Storage & Disposal of Fuel	• MS001-Provide Inventory Management • MS002 Procure Materials • MS003-Procure Contract Services • MS004-Provide Warehousing • MS005-Repairs, Refurbishment & Returns • MS006-Inventory Disposal	• T001-Develop Training Programs • T002-Conduct Training • T003 Attend Training	• LP001 Provide Security Measures • LP002-Provide Performance Monitoring & Improvement Services • LP003-Provide Safety Services • LP004 Maintain License & Permits • LP005-Perform Emergency Planning • LP006 Provide Fire Protection	• SS001-Provide Information Technology Services • SS002-Provide Business Services (includes Nuclear Asset Management) • SS003-Provide Information Management Services • SS004-Provide Human Resources Services • SS005-Maintain Grounds, Facilities & Vehicles • SS006-Support Community & Government Relations • SS007-Support Nuclear Industry, Professional & Trade Associations

Figure 39 - Standard Nuclear Performance Model - Sub-processes [41]

7.4.3 Organizational View

Figure 40 shows the major programmes that must be implemented to operate a nuclear power plant based on [42]. The organizational structure does not need to exactly match these programmes but must provide coverage such that there is an Organizational Unit responsible for each programme.

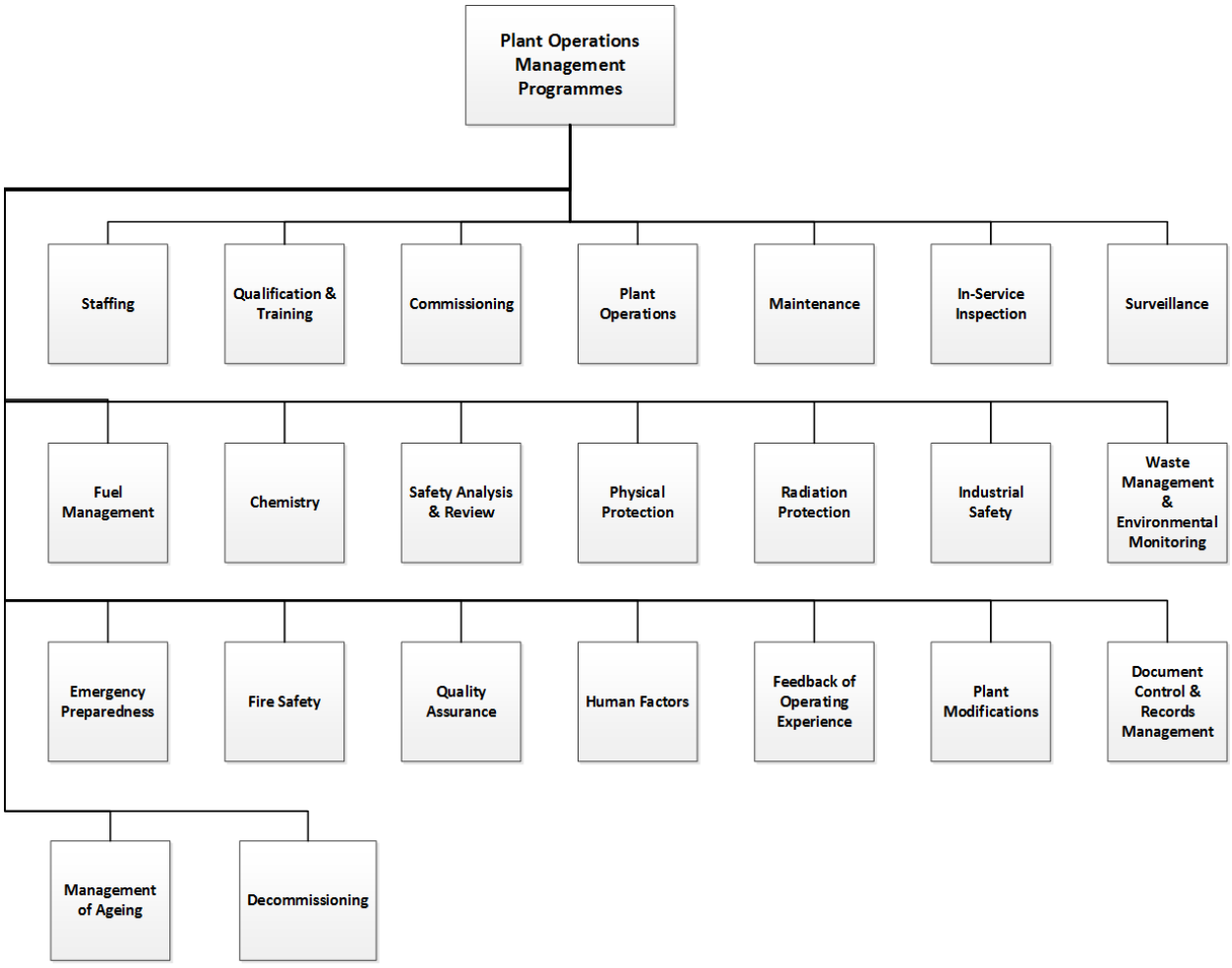


Figure 40 - Programmes Required to Operate a Nuclear Power Plant [42]

7.4.4 Safety Control Structure View

Figure 41 shows a high level safety control structure for a nuclear power utility. Enterprise Objects provide direction and feedback for the Business Processes that design, operate, maintain, modify and monitor the nuclear power plant.

The governance box represents the Decision Centres that give direction to the Business Processes.

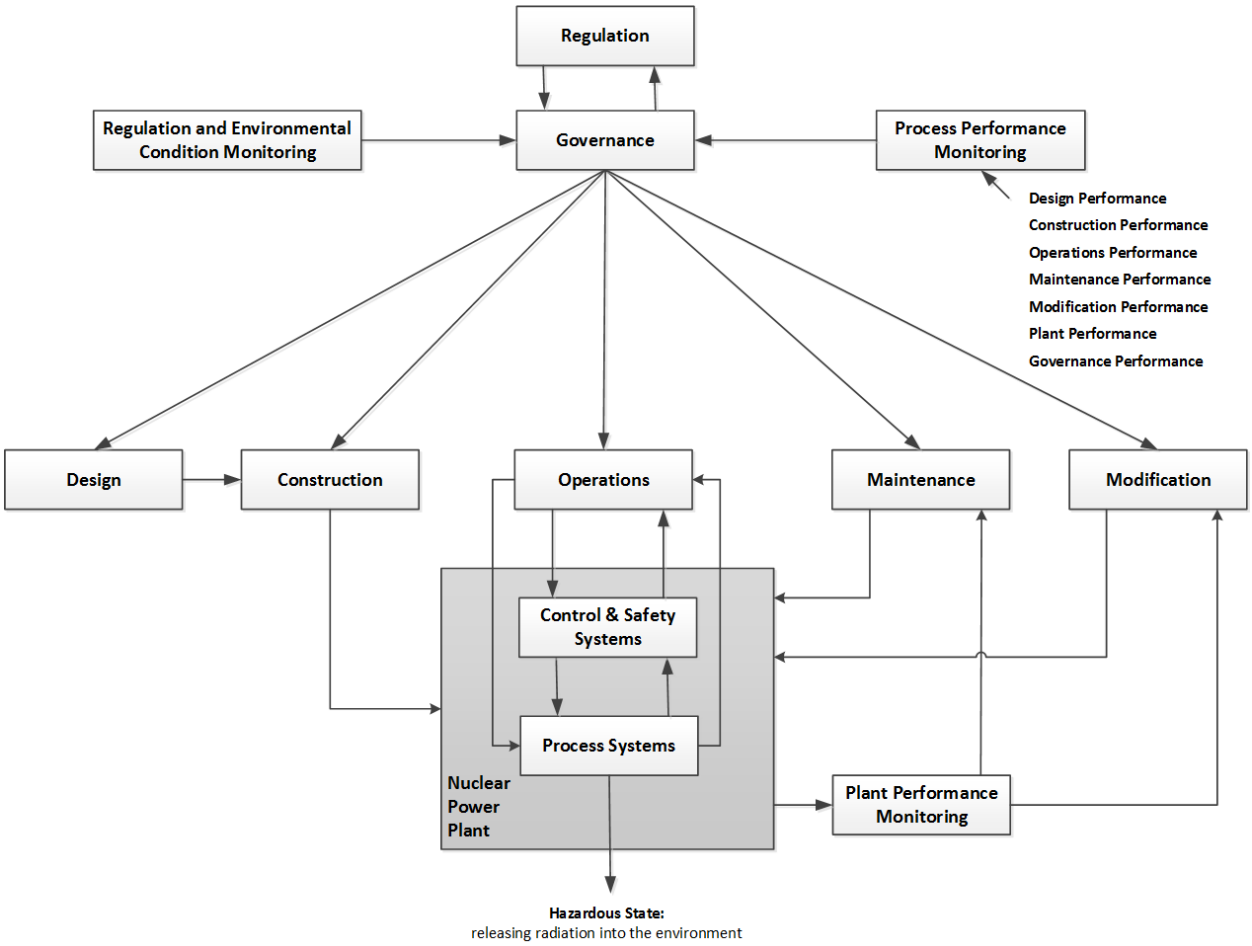


Figure 41 - Nuclear Power Utility: Safety Control Structure

8 NUCLEAR BEST PRACTICE

Chapter 5 of the thesis outlined the process to be applied to engineer an enterprise (both the hazardous technology and the business processes, organizations and governance that design, construct, operate and maintain the hazardous technology). Chapter 7 defines some models that represent the products from the safety enterprise engineering process. This Chapter of the thesis defines a set of principles that should be true in order to achieve a safety goal. The principles were identified by reverse engineering them from nuclear best practice documents that are available in the public domain.

There are many requirements that must be satisfied in order to achieve a well run, effective enterprise. The focus of the thesis is on those requirements associated with achieving a safety goal. To maintain the focus on safety, the initial focus is on the requirements on the potentially hazardous technology to achieve safety. Then the focus is expanded to requirements on the business processes, organization and governance that are necessary to achieve the requirements on the hazardous technology. These requirements are examined for the design and construction phase and then the operations and maintenance phase of the enterprise. During both phases there is a requirement for performance monitoring and continuous improvement to keep risks as low as reasonably achievable, and to avoid degradation of safety over time. The requirements on performance monitoring and continuous improvement are therefore examined separately. As described in Chapter 4, safety is a function of the technology being in a hazardous state and the environment being in a worst case state relative to the hazardous state. Therefore, requirements on the environment are also examined.

The chapter is structured as follows:

- Section 8.1 outlines the nuclear best practice documents that exist and those that were selected to be the basis of the reverse engineering efforts.
- Section 8.2 describes the reverse engineering process and the structure of information that was used to provide traceability from generalized principles to the specific nuclear industry requirements.
- Section 8.3 describes the principles associated with the dangerous technology for which the enterprise is responsible.
- Sections 8.4 through 8.7 describe the principles associated with business processes, organizations and governance.

- Section 8.4 describes the principles associated with the design and construction phase.
- Section 8.5 describes the principles associated with the operations and maintenance phase.
- Section 8.6 describes the principles associated with performance monitoring and continuous improvement.
- Section 8.7 describes the principles associated with the environment (natural environment, technological environment and social environment).

Appendix 3 contains the detailed principles based on the source documents. Sections 8.3 through 8.7 contain summaries of the detailed principles in Appendix 3. The summaries were produced by grouping the detailed principles by the area they primarily impact (technology, business process, organization or governance) and the lifecycle phase that they primarily impact (design and construction vs operation and maintenance). The resulting groups of principles were then examined for common themes reflected in the detailed principles and these were then summarized in sections 8.3 through 8.7.

8.1 Nuclear Best Practice Documents

The nuclear industry has a very structured and comprehensive set of documents created and maintained by industry associations to capture and share best practices among nuclear industry utilities. It has been realized that members of the industry must help each other achieve nuclear safety since the failure of any one member has significant consequences to all members of the industry by undermining public confidence.

The International Atomic Energy Agency (IAEA) publishes a set of safety standards which capture the fundamental principles, requirements and recommendations to ensure nuclear safety. Figure 42 shows the structure of the set of safety standards.

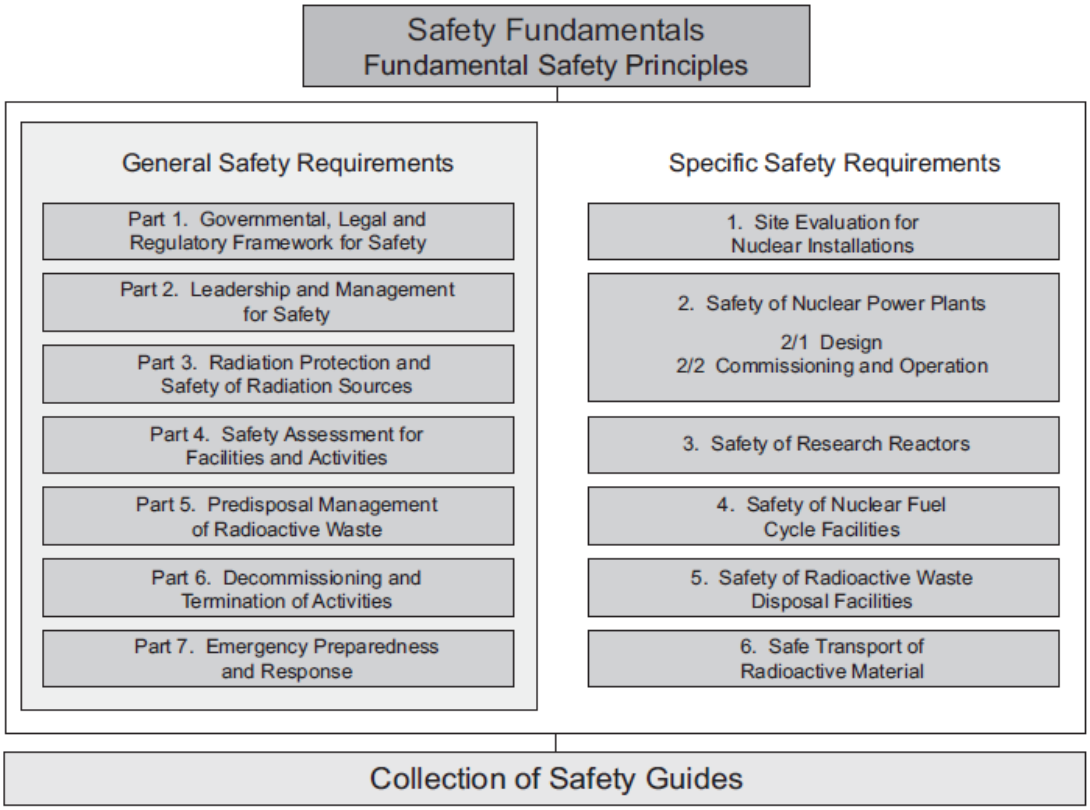


Figure 42 - IAEA Safety Standards [55]

Key documents within this set of best practice documents are those that capture requirements necessary to achieve nuclear safety. The following documents were identified as being the best source of material to reverse engineer principles for achieving safety.

1) International Atomic Energy Agency, and Euratom, eds. 2006. *Fundamental Safety Principles* [43]
2) International Nuclear Safety Advisory Group, and International Atomic Energy Agency, eds. 1999. *Basic Safety Principles for Nuclear Power Plants* [44]
3) Defence in Depth in Nuclear Safety: A Report. 1996. INSAG 10. International Atomic Energy Agency [45]
4) International Atomic Energy Agency. 2016. *Safety of Nuclear Power Plants: Design* [31]
5) International Atomic Energy Agency. 2016. *Safety of Nuclear Power Plants: Commissioning and Operation* [32]
6) International Atomic Energy Agency. 2016. *Leadership and Management for Safety* [46]

7) International Atomic Energy Agency. 2016. *Governmental, Legal and Regulatory Framework for Safety*

These set of document provide coverage of key principles (1, 2 and 3), requirements for the design, commissioning and operations phases of the plant lifecycle (4 and 5), requirements on the leadership and management (6) and a requirements on the governmental, legal and regulatory framework necessary to achieve and maintain safety (7).

8.2 Reverse Engineering Principles from Best Practice Documents

As discussed in Chapter 5 on Safety Enterprise Engineering, the achievement of safety requires that hazards be identified, potential causes of the hazards be identified and design features be incorporated into the design to eliminate, control or mitigate the potential causes of the hazards.

The principles and requirements in the source IAEA documents were reviewed and for each requirement an assessment was done to determine the underlying cause of hazard and design feature that the principle or requirement was derived from. The resulting causes and design features were generalized from the nuclear specific principles and requirements to attempt to derive results that could be applied outside of the nuclear power domain.

The results were grouped first by phase (design and construction vs operations and maintenance phase) and then by whether they impacted the technological system (power plant), the business processes, the organization or governance. This grouping helped focus the principles on the different design views of the enterprise necessary to achieve safety.

Figure 43 shows the structure that was used to document and assess each principle and requirement.

Requirement	Hazard Addressed by Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with Cause
The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design.	Unsatisfied safety requirement	too high a likelihood that errors are introduced into the design that impact satisfaction of safety requirements too low a likelihood that errors in the design that impact satisfaction of safety requriements are detected	use of proven processes and methods for the engineering of the system as defined in appropriate codes and standards controlling changes to the design to ensure assurance that safety requirements are satisfied is maintinaed at the same level or better when changes are made to the design independent personnel perform V&V activities
Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards.	Unsatisfied safety requirement	use of items that do not have adequate supporting evidence that they are fit for purpose Lacking adequate: - operating history - use of applicable codes and standards in its engineering - test results - research results - in service monitoring of its performance	qualification process compliant with appicable codes and standards
Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process for a nuclear power plant to ensure that all safety requirements on the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design, as delivered, meets requirements for manufacture and for construction, and as built, as operated and as modified.	Unsatisfied safety requirement Operation outside of safe Operating Envelope Introduction of new hazard via modification requiring new/modified safety requirement that is not satisfied by existing design	too low a likelihood that errors in the design that impact satisfaction of safety requriements are detected Operator performance inconsistent with performance assumed by the design Design change introduced new hazard that was not detected and confirmed to be addressed adequately by design	use of proven processes and methods for the engineering of the system as defined in appropriate codes and standards controlling changes to the design to ensure assurance that safety requirements are satisfied is maintinaed at the same level or better when changes are made to the design independent personnel perform V&V activities clear documentation of safe operating envelope and its incorporation into operating procedures

Figure 43 - Reverse Engineering from IAEA Requirements

The resulting causes of hazards and design features were then grouped as shown in Figure 44.

The following sections show the design features that are applicable to each view of the enterprise (technical, business process, organizational and governance) at each lifecycle stage (design and construction vs operation and maintenance). The design features shown were derived from Appendix 3 by looking at the design features applicable to each view and phase, and then grouping them by common themes.

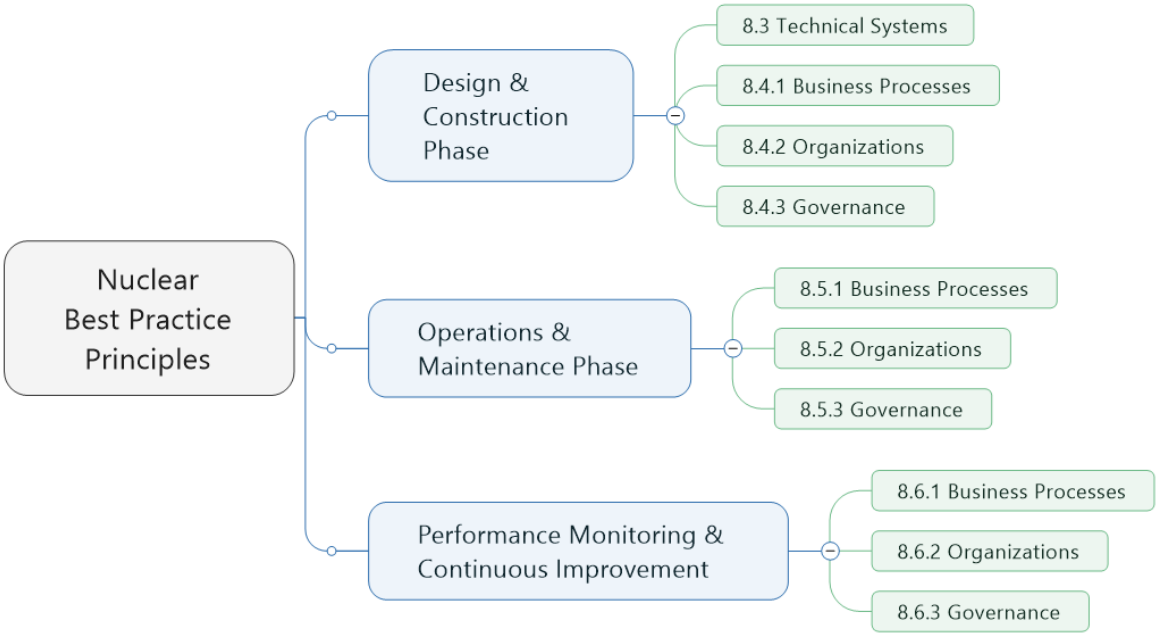


Figure 44 - Grouping of Reverse Engineering Results

Appendix 3 has the tables of principles, requirements and resulting causes of hazards and design features.

8.3 Technical System Design Principles

The safety design principles for a nuclear power plant are known as the defence in depth principles. This section provides a historical summary of the development of these defence in depth principles (section 8.3.1) and a summary description of the principles (section 8.3.2). The detailed principles are listed in Appendix 3.

8.3.1 Historical Development of Defence in Depth Principles

"Historically, nuclear safety was achieved by applying the concept of placing multiple barriers between radioactive materials and the environment. The concept of defence in depth was gradually refined to constitute an increasingly effective approach combining both prevention of a wide range of postulated incidents and accidents and mitigation of their consequences. Incidents and accidents were

postulated on the basis of single initiating events selected according to the order of magnitude of their frequency, estimated from general industrial experience." [45]

The approach was intended to provide redundant means to ensure the fulfilment of the basic safety functions of controlling the power, cooling the fuel and confining radioactive material (Control, Cool and Contain).

In its early stage, the concept of defence in depth generally included three levels:

— conservative design, providing margins between the operating conditions foreseen (covering normal operation as well as postulated incidents and accidents) and the failure conditions of equipment;
— control of operation, including response to abnormal operation or to any indication of system failure, by the use of control, limiting and protection systems to prevent the evolution of such occurrences into postulated incidents and accidents;
— engineered safety features, to control postulated incidents or accidents in order to prevent them from progressing to severe accidents or to mitigate their consequences, as appropriate.

Later, the concept of defence in depth was further refined to include consideration of external hazards, quality assurance, automation, monitoring and diagnostic tools. Furthermore, additional severe accidents were considered in studies and probabilistic safety analyses.

The Three Mile Island accident in the United States of America in 1979, which led to a severe core melt, bore out many of the results of the first theoretical studies of severe accidents and probabilistic safety analyses. The accident illustrated the importance of human factors, the human-machine interface and long term effective containment. It resulted in advances in the physical understanding of potential severe accidents due to extensive research work. Moreover, it demonstrated the importance of effective analysis and feedback of operating experience, to identify and eliminate possible weaknesses in defence in depth, including weaknesses in design, operating procedures and training.

Feedback of experience and investigation of severe accidents resulted in new extensions of the concept of defence in depth:

— additional measures were introduced in order to cope with significant multiple failures such as a complete loss of redundant systems;
— accident management was implemented in order to prevent accidents or, in the event of non-postulated accidents, to mitigate their consequences;
— symptom oriented emergency procedures were developed;
— provision was made for on-site and off-site emergency response to mitigate the effects on the public and the environment of the release of radioactive materials.

The Chernobyl accident in 1986 demonstrated the possible consequences of inadequate defence in depth and the importance of organizational issues such as the need for an effective regulatory regime and for a safety culture. It also focused attention on medium and long term contamination due to radioactive releases and the role of off-site emergency planning.

The requirements for the application of the defense in depth strategy are documented in [45]. The requirements are also embedded within the other IAEA documents that were used as the basis for reverse engineering as described in Section 8.1.

The defence in depth requirements are organized around five “levels” of defence as follows

Level 1) Prevention of abnormal operations and failures

Level 2) Control of abnormal operation and detection of failures

Level 3) Control of accidents within the design basis

Level 4) Control of severe plant conditions

Level 5) Mitigation of consequences of significant releases of radioactive materials

The first level strives to prevent the plant from going into a hazardous state by preventing failures and preventing abnormal operations. This is achieved by using conservative design, high quality of construction, and high quality of operation. The intent is to make deviations from normal operations infrequent.

The second level incorporates design features to deal with anticipated operational occurrences and failures. These design features work to bring the plant back to normal operating conditions as soon as possible. The design features include control systems, protection systems and other surveillance features.

The design features that are part of level 3 are called upon if the first two levels fail and accident conditions occur. The level 3 features strive to prevent evolution towards severe accidents and to confine radioactive materials within the containment system. The features are implemented by engineered safety features and accident procedures.

Level 4 features give consideration to severe plant conditions that were not explicitly addressed in the design of level 1, 2 and 3 features due to their very low probability of occurrence. The level 4 features strive to ensure that the likelihood of an accident entailing severe core damage, and the magnitude of radioactive material releases in the unlikely event of a severe plant condition are both kept as low as reasonably achievable. Level 4 features include ancillary and support systems, and measures for accident management.

Level 5 features strive to limit the consequences of severe accidents. The level 5 features deal with off-site emergency procedures and preparedness.

Common to all five levels are principles around conservatism, quality assurance and safety culture.

Figure 45 provides a graphical representation of the layers of defense. Each circle represents a state of the plant with normal operations in the center and harm to people occurring in the outermost circle. Each level of defense is focused at preventing a state transition from a lower severity state to a higher severity state.

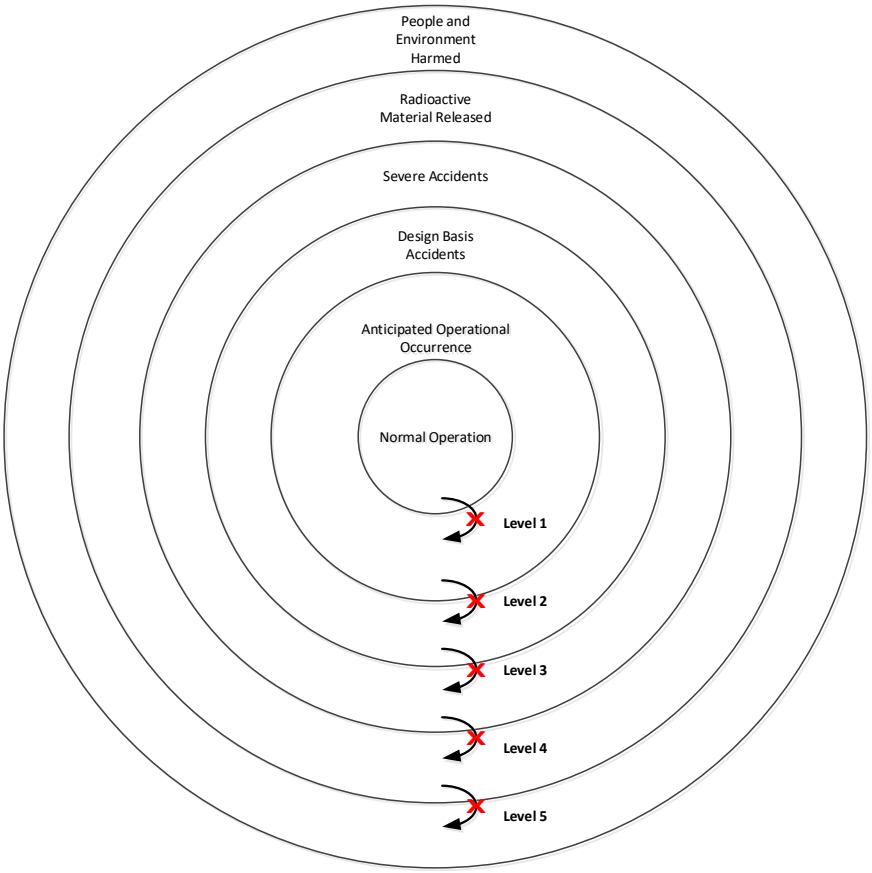


Figure 45 - Defence in Depth Layers

8.3.2 Technical Principles Based on Defence in Depth Strategy

Appendix 3 lists the requirements in the documents listed in Section 8.1 and groups them as discussed in Section 8.2.

This section summarizes the requirements associated directly with the design of the nuclear power plant (the technical system).

As discussed in Section 8.3.1, nuclear safety is achieved primarily through the implementation of a defence in depth strategy consisting of five levels of defence. The following Sections summarizes the design features in Appendix 3 impacting the technical design necessary to achieve each of the five levels.

8.3.2.1 Level 1 Principles

Level 1: prevent the plant from going into a hazardous state by preventing failures, and preventing abnormal operations.

The safety provisions at Level 1 are taken through the choice of site, design, manufacturing, construction, commissioning, operating and maintenance requirements. The relevant requirements are:

- Design systems containing radioactive material to prevent occurrence of events that could lead to uncontrolled release to the environment, prevent overheating, to contain releases of radioactive material and to facilitate mitigation of radiological consequence in accident conditions.

- Design satisfies all regulatory requirements and applicable national and international standards.
- Design utilizes defense-in-depth principle to achieve control, cool and contain with a high degree of confidence.
- Use of proven designs, compliant with applicable national and international standards with adequate demonstration of achievement of safety requirements.
- Systematic approach to design plant to satisfy control, cool and contain.
- Design means to monitor compliance with control, cool and contain.

- To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment.
- The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves.
- Designed to cope with a set of events including normal conditions, anticipated operational occurrences, extreme external events and accident conditions.
- For this purpose, conservative rules and criteria incorporating safety margins are used to establish design requirements.
- Comprehensive analyses are carried out to evaluate the safety performance or capability of the various components and systems in the plant.

- The core is designed to have mechanical stability.

- It is designed to tolerate an appropriate range of anticipated variations in operational parameters.
- The core design is such that the expected core distortion or movement during an accident within the design basis would not impair the effectiveness of the reactivity control or the safety shutdown systems or prevent cooling of the fuel.

- Heat transport systems are designed for highly reliable heat removal in normal operation.
- They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur.
- Components, structures, and systems used during startup, low power and shutdown operations are designed to maintain or restore the reactivity control, decay heat removal, and the integrity of the fission product barriers, so as to prevent the release of radioactive material resulting from accidents initiated during those operations.

- A set of operational limits and conditions is defined to identify safe boundaries for plant operation. Minimum requirements are also set for the availability of staff and equipment.
- Design takes into account applicable operating experience.

- The safety functions of systems important to safety are designed to not be impacted by disturbances of the power grid.

- Design access controls to the plant.
- Design system important to safety to prevent unauthorized access.

- Design takes into account choice of materials so that the amount of radioactive waste generated is minimized to the extent practicable
- Design to prevent processes that transport radioactive material external to the plant.
- Radiation protection features are incorporated to protect plant personnel from radiation exposure and to keep emissions of radioactive effluents within prescribed limits.
- Design includes facilities to manage radioactive waste
- Plant designs provide for the handling and storage of new and spent fuel in such a way as to ensure protection of workers and to prevent the release of radioactive material.

8.3.2.2 Level 2 Principles

Level 2: deal with anticipated operational occurrences and failures

- The design shall take into account measures that prevent accidents and mitigate the consequences of accidents that do occur.
- The design takes into account interactions between systems to ensure that failures of systems providing redundant or diverse safety functionality do not have common cause failures.
- Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent of the equipment and processes used to control the reactor power.
- Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally.

8.3.2.3 Level 3 Principles

Level 3: prevent evolution towards severe accidents and to confine radioactive materials within the containment system

- Design ensures that the risk of radiological accidents is as low as reasonably practical.

- Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents.
- Provision is made for alternative means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost.

- Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.

- Consider opportunities for increasing safety utilizing capabilities of multi-unit stations in the design

- Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which the main control room may be uninhabitable or damaged.
- The control room is designed to remain habitable under normal operating conditions, anticipated abnormal occurrences and accidents considered in the design.

8.3.2.4 Level 4 Principles

Level 4: ensure that the likelihood of an accident entailing severe core damage, and the magnitude of radioactive material releases in the unlikely event of a severe plant condition are both kept as low as reasonably achievable

- The plant is designed to be capable of retaining the bulk of the radioactive material that might be released from fuel, for the entire range of accidents considered in the design.
- The results of an analysis of the response of the plant to potential accidents beyond the design basis are used in preparing guidance on an accident management strategy.

- If specific and inherent features of a nuclear power plant would not prevent detrimental effects on the confinement structure in a severe accident, special protection against the effects of such accidents is provided, to the extent needed to meet the general safety objective.
- Equipment, instrumentation and diagnostic aids are available to operators, who may at some time be faced with the need to control the course and consequences of an accident beyond the design basis.
- Design suitable communications systems to be able to communicate to personnel during operations and during an emergency with sufficient redundancy and diversity.

- Means are available to the responsible site staff to be used in early prediction of the extent and significance of any release of radioactive

materials if an accident were to occur, for rapid and continuous assessment of the radiological situation, and for determining the need for protective measures.

8.3.2.5 Level 5 Principles

Level 5: limit the consequences of severe accidents

- Emergency plans are prepared before the startup of the plant, and are exercised periodically to ensure that protection measures can be implemented in the event of an accident which results in, or has the potential for, significant releases of radioactive materials within and beyond the site boundary. Emergency planning zones defined around the plant allow for the use of a graded response.
- It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.

- A permanently equipped emergency centre is available off the site for emergency response.
- On the site, a similar centre is provided for directing emergency activities within the plant and communicating with the off-site emergency organization.

- Design sufficient escape routes meeting national and international standards.

8.4 Design and Construction Phase Principles

During the design and construction phase, the potentially dangerous technology is first designed and then built. Effective achievement of the technical design principles listed in Section 8.3.2 above are dependent upon the business processes, organizations and governance utilized to perform design and construction. The following Sections summarize the principles impacting the business process, organizational and governance design of the enterprise.

8.4.1 Business Process Related Principles

The design features impacting the business processes during the design and construction phase can be grouped into the following areas:

- Design process
- Documentation
- Programs
- Safety management

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.4.1.1 Design Process

The design process related design features are:

- Design process consistent with industry best practice
- Use of proven processes and methods for the engineering of the system as defined in appropriate codes and standards
- Technical specifications for items important to safety shall be developed using appropriate methods that result in complete and correct specifications of safety requirements.
- Use of effective hazard analysis techniques
- Controlling changes to the design to ensure assurance that safety requirements are satisfied is maintained at the same level or better when changes are made to the design
- Establishment of a design modification process that is compliant with relevant national and international standards, and is based on proven engineering practices
- Establishment of controls of the interfaces between responsible designers and suppliers engaged in design work

- The design of items important to safety shall take into account the attributes of manufacturability, constructability and installabilty to ensure that the probability of introduction of undetected errors is commensurate with the level of risk of errors.
- Operating experience from the design, construction and operation of similar plants shall be taken into account.
- The design and verification processes take into account ageing and wearout mechanisms
- Design modification process includes proper design and safety reviews, implementation and testing
- HMI supports achievement of operations and maintenance performance assumed in the design
- Design margins established to account for unanticipated failures.
- Security measures designed into systems to mitigate risks from security threats
- Establish mechanisms to manage any potential conflicts between safety and security measures
- Establish fire hazard analysis as part of the overall plant hazard analysis
- Establish a supplementary control room

8.4.1.2 Documentation

The documentation related design features are:

- Clear documentation of safe operating envelope and its incorporation into operating procedures
- Assumptions on operations and maintenance performance necessary to achieve safety is clearly documented
- Clear documentation of the engineering process

8.4.1.3 Programs

The programs related design features are:

- Establish and implement a program for the qualification, selection, evaluation, procurement and oversight of the supply chain
- Qualification programme complies with appropriate industry standards
- Qualification process compliant with applicable codes and standards
- The qualification of procured items shall include a hazard analysis to determine if there are any new hazards introduced by the use of the item
- Procured items important to safety shall be qualified as being compliant with safety requirements
- An effective ageing management is in place that monitors for ageing mechanisms and unanticipated behaviour of systems
- Comprehensive commissioning program addressing all safety related requirements
- Comprehensive commissioning program addressing all safety related operating procedures

8.4.1.4 Safety management

The safety management related design features are:

- A safety analysis shall be performed and documented providing traceable evidence that the system will satisfy its safety requirements
- The safety analysis shall document the assumptions upon which it is based and the uncertainties upon which the design margins are based.
- Compliance of safety management plan with industry standards

- The safety management system shall be integrated into the overall management system
- Assessments and audits of compliance with safety management plan
- Documented safety management plan

8.4.2 Organization Related Principles

The design features impacting the organization during the design and construction phase can be grouped into the following areas:

- Competencies
- Organizational Structure
- Management system

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.4.2.1 Competencies

The competency related design features are:

- Competencies required for each design activity are clearly defined
- Well documented competencies required for the performance of each design process
- Use of competent personnel to perform hazard analysis
- Competent personnel perform design and verification activities
- Qualification is performed by competent personnel
- Competent personnel planning and executing the commissioning program

- Comprehensive training of personnel in the expectations of the engineering process
- Understanding of all personnel on their role in the safety management plan

8.4.2.2 Organizational Structure

The organizational structure related design features are:

- Independent personnel perform V&V activities
- Design of operations and maintenance organizations are consistent with design assumptions on operations and maintenance performance
- Operations and maintenance personnel are involved in effective design reviews to ensure that assumptions on operations and maintenance performance are achievable
- Clear accountability for the establishment of a safety management system

8.4.2.3 Management system

The management system related design features are:

- Documented assessments of personnel demonstrating required competencies for tasks/processes assigned to them
- The management system shall ensure that personnel assigned to design activities have the pre-requisite competencies to perform those activities

8.4.3 Governance Related Principles

The design features impacting governance during the design and construction phase can be grouped into the following areas:

- Expectations

- Management

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.4.3.1 Expectations

The expectations related design features are:

- Well documented expectations for the design process
- Clearly established expectations on the leadership to communicate, demonstrate and reinforce the expected safety behaviour
- Expectation that safety goals are periodically reviewed against organizational strategies and plans are established
- Expectation for effective communications and interactions with interested parties about safety is established
- Expectations that the safety management system be developed, applied and continuously improved shall be established.
- Establishment of clear expectations on the documentation, revisions control and communication of the safety management system
- Clearly established policy and governance with respect to the expectations for taking safety into account in all decisions
- Criteria are established to grade the development and application of the management system taking into account the safety significance of decisions

8.4.3.2 Management

The management related design features are:

- Adequate schedule and resources provided to perform design processes in accordance with expectations
- Clear and measurable safety goals are established at various levels in the organizations
- Effective management oversight of the engineering process

8.5 Operations and Maintenance Phase Principles

During the operations and maintenance phase, the potentially dangerous technology must be operated within its safe operating envelope and maintained to achieve ongoing compliance with established safety requirements. Effective achievement of the technical design principles listed in Section 8.3.2 above are dependent upon the business processes, organizations and governance utilized to perform operations and maintenance. The following Sections summarize the principles impacting the business process, organizational and governance design of the enterprise.

8.5.1 Business Process Related Principles

The design features impacting the business processes during the operations and maintenance phase can be grouped into the following areas:

- Configuration management
- Programs for:
  - Training
  - Commissioning
  - Ageing management
  - Maintenance
  - Radioactivity management
  - Fire safety
  - Chemistry
  - Housekeeping
  - Non- safety related

- Management
- Emergency Preparedness

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.5.1.1 Configuration management

- Establishment of controls over the configuration of the physical plant and its design
- Establishment of controls over the configuration of the physical plant and its design including a limit on the number of temporary modifications and limits on the time they may be in effect
- Establishment of controls on plant configuration that ensures changes to plant configuration are consistent with the established safe operating envelope
- Establish a system of controls for records and reports related to safety related maintenance and surveillance

8.5.1.2 Programs

8.5.1.2.1 Training Program

- Establishment of a program to establish the necessary competencies required within the operating organization and the development and training program to maintain the required competencies
- Establish training programs to ensure that all personnel understand their responsibilities with respect to safety
- Establish training programs on the use of the supplementary control room

- Personnel development program that ensures personnel have the necessary competencies to perform safety related activities assigned to them
- Programs to communicate and train personnel in the safety policies
- A training program is established to ensure that personnel assigned safety related activities are knowledgeable of the operating limits and conditions
- Programs to educate personnel their role in achieving and maintaining safety

8.5.1.2.2 Commissioning Program

- Establish operating and maintenance procedures necessary to keep the plant operating within its safe operating envelope and validate the procedures as part of the commissioning program
- Establish and implement a commissioning program that demonstrates that the plant as built is compliant with all design assumptions and licensing conditions
- Establish a decommissioning plan

8.5.1.2.3 Ageing management

- Establish an ageing management program to maintain the performance of structures, systems and components that have an impact on safety

8.5.1.2.4 Maintenance

- Establish and implement a program for the planning and execution of online and offline maintenance and design modification activities
- Establish a maintenance program to keep the supplementary control room functional

- Establish a maintenance program for all equipment that is related to performing safety functions in the plant
- Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements
- Robust technical justification for the inspection and maintenance program.
- Establishing a program of surveillances, inspections and audits to verify compliance with safety related governance programs

8.5.1.2.5 Radioactivity management

- Establish operating practices that keep generation of radioactive waste to a minimum
- Establish and implement a radioactive waste management program to manage the processing, transport, storage and disposal of radioactive waste
- Establish a non-radiation-related safety program and integrate it into the radiation-related safety program
- Establish and implement a safe reactivity management program

8.5.1.2.6 Fire safety

- Establish and implement a fire safety program
- Establish procedures, equipment and staffing to coordinate with firefighting services

8.5.1.2.7 Chemistry

- Establish and implement a chemistry program

8.5.1.2.8 Housekeeping

- Establish a housekeeping program to ensure that operational premises and equipment are maintained, well lit and accessible

8.5.1.2.9 Non- safety related

- Establish non-safety related programs taking into account any potential impacts to safety related equipment or activities

8.5.1.3 Management

- Establishment and use of a management system that ensures that the plant is operated in a safe manner and within the safe operating envelope
- Establish policies for scheduling of personnel for safety related activities to ensure that sufficient time is allocated to adequately perform the activities
- Establish a staff health policy that ensures staff are fit for duty

8.5.1.4 Emergency Preparedness

- Establishment of a comprehensive emergency plan for responding to a nuclear or radiological emergency
- Establishment of a training program so that personnel have the necessary competencies to execute the emergency plan in response to an accident
- Establishment of, and maintenance of the facilities and equipment necessary to execute the emergency plan in response to an accident

- Establishment of an accident management program that covers preparatory measures, procedures, guidelines and equipment necessary for preventing the progression of accidents and mitigating the consequences of accidents.
- Competent personnel and supporting equipment necessary to deal with accidents including concurrent accidents.
- Contingency measures including alternative supply of cooling water and alternate supply of electrical power.
- Accident management program that takes into account the possibility of regional infrastructure being degraded and of adverse working conditions, as well as the possibility that operating conditions for equipment will be degraded.

8.5.2 Organization Related Principles

The design features impacting the organization during the operations and maintenance phase can be grouped into the following areas:

- Competencies
- Organizational Structure

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.5.2.1 Competencies

- Clear definitions for the qualifications and competencies of personnel assigned to safety related activities are documented.
- Establish a program to ensure personnel assigned to safety related activities have the necessary competencies to perform the activities assigned to them

- Establishment of a training program that ensures that personnel assigned to safety related tasks have the necessary qualifications and competencies
- Establishment of a continuous improvement program for the training program
- Governance for assigning personnel to safety related tasks includes confirmation that the personnel have the necessary qualifications and competencies
- Establish a staffing plan that ensures that sufficient competent staff are available to perform safety related activities

8.5.2.2 Organizational Structure

- documentation of functional responsibilities, lines of authority, and lines of communications for all safety related activities
- Establishment of the necessary organizational structures for managing and emergency
- Clear responsibility for the safety of the plant within the operating organization's management system
- Clear responsibility for overall responsibility of design integrity
- Clear definition of accountabilities for managers responsible for the safety of the plant during siting, design, construction, commissioning, operation and decommissioning.

8.5.3 Governance Related Principles

The design features impacting governance during the operations and maintenance phase can be grouped into the following areas:

- Safety Management
- Emergency Preparedness

- Configuration management
- Safety culture

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.5.3.1 Safety Management

- Safety management system
- Establishment of a safety management system that establishes safety goals, strategies, plans and objectives including their measurement and review to identify necessary actions to deal with deviations
- Establishment of a safety management system that takes into account the safety significance of changes
- Establishment of a safety management system that is clearly documented
- Integration of the safety management system into the management system of the organizations
- Safety policies establishing the priority for safety and the standards to be met for all safety related activities
- Clear policies and governance defining responsibilities for safety related activities
- Management of responsibilities and interfaces between safety related activities, especially when involving off-site organizations and contractors.
- Clear definition of the accountability of senior managers for establishing an effective safety management system
- Establishing processes, organizations and governance in compliance with standards for safety, quality and management.

- A complete set of operating limits and conditions are documented and consistent with design assumptions and intent
- Establishing governance that ensures adequate resources and funding are available to achieve and maintain safety including during decommissioning and for radioactive waste disposal
- Establishment of a program for identification and effective communication with parties interested in the safety of the plant
- Establishment of governance that focuses on optimizing safety by keeping radiation risks as low as reasonably achievable

8.5.3.2 Emergency Preparedness

- Establishment of an adequate emergency preparedness program.

8.5.3.3 Configuration management

- Establishment of a document and records management system so that all safety related documents are controlled and the correct version of documents and records are available to personnel requiring them

8.5.3.4 Safety culture

- Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety
- Clearly defined responsibilities for all managers to advocate and support a safety culture
- Establishment of governance that focuses on optimizing safety by establishing a safety culture throughout the organization

8.6 Performance Monitoring and Continuous Improvement Principles

During both phases (design and construction, and operations and maintenance) there is a requirement for performance monitoring and continuous improvement to keep risks as low as reasonably achievable, and to avoid degradation of safety over time. The following Sections summarize the principles impacting the business process, organizational and governance design of the enterprise.

8.6.1 Business Process Related Principles

The design features impacting business processes for performance monitoring and continuous improvement can be grouped into the following areas:

- Safety Management
- Programs

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.6.1.1 Safety Management

- Establish a safety management system that ensures the continuing safety of the plant design.
- Establishment of a leadership for safety program
- Effective review of processes to ensure that safety consequences are taken into account within each process, and in the interactions between processes

- Establish continuous improvement process taking input from periodic safety review and operational experience both internal and external to the organization
- Establish periodic safety reviews of the plant, processes, organizations and governance
- Effective documentation of processes that is maintained as configuration items in a configuration management program
- Review, monitoring and assessment of safety related activities on a regular basis
- Continuous improvement program focused on operational safety
- Periodic safety review program including review of operational experience inside and outside the organization

8.6.1.2 Programs

- Establishment of a set of programs necessary to achieve and maintain safety along with the establishment of an effective management system for the programs
- Establishment of a risk management program that ensures that risks are identified, analyzed and reduced to levels as low as reasonably achievable.
- Establish an audit and review program to ensure that the safety management program has been effectively implemented and continuously improved over time
- Effective equipment qualification programs to provide confidence that equipment will satisfy its safety requirements
- Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner.
- Establish a program to investigate events with significant implications for safety and take effective actions to avoid reoccurrence of the events.

- A continuous improvement program is established that revises operating limits and conditions based on operating experience
- A monitoring and surveillance program is established that detects deviations from operating limits and conditions, and takes appropriate remedial actions

8.6.2 Organization Related Principles

The design features impacting organizations for performance monitoring and continuous improvement can be grouped into the following areas:

- Competencies
- Organizational Structure

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.6.2.1 Competencies

- Competencies required for each design activity are clearly defined
- The management system shall ensure that personnel assigned to design activities have the pre-requisite competencies to perform those activities

8.6.2.2 Organizational Structure

- Designate an individual to be responsible for the safety of the plant design
- Establish the organization responsible for audit and review to have sufficient authority and organizational independence to be able to identify

problems, to recommend solutions and to verify that solutions have been effectively implemented.

8.6.3 Governance Related Principles

The design features impacting governance for performance monitoring and continuous improvement can be grouped into the following areas:

- Safety Management
- Expectations

The following sections list the applicable design features from Appendix 3 grouped by these areas.

8.6.3.1 Safety Management

- Establish accountabilities for senior management to establish and implement a safety management program
- Establish accountabilities for managers to support and advocate a strong safety culture
- The safety management system shall be integrated into the overall management system
- Clear and measurable safety goals are established at various levels in the organizations
- Expectation that safety goals are periodically reviewed against organizational strategies and plans are established
- Criteria are established to grade the development and application of the management system taking into account the safety significance of decisions

8.6.3.2 Expectations

- Establishment of clear expectations on the documentation, revisions control and communication of the safety management system
- Clearly established expectations on the leadership to communicate, demonstrate and reinforce the expected safety behaviour
- Expectations that the safety management system be developed, applied and continuously improved shall be established.
- Clearly established policy and governance with respect to the expectations for taking safety into account in all decisions
- Expectation for effective communications and interactions with interested parties about safety is established

8.7 Principles Associated with the Environment

An accident occurs due to the combination of the system (enterprise) being in a hazardous state and the environment being in a worst case state relative to the hazardous state of the system. The environment can be partitioned into the natural environment, the technological environment and the sociological environment as illustrated in Figure 25.

The following sections list principles applicable to the sociological portion (laws and regulation) of the environment, and its business processes, organization and governance.

8.7.1 Business Process Related Principles

The design features relevant to the business processes of the sociological portion of the environment are:

- Analyze Operating and Regulatory Experience and Disseminate Lessons Learned
- Management System in Regulatory Body to Effectively Perform Regulation
- Formal and Informal Communication with Licensees
- Regulatory Body Must Authorize Each Facility Before Operation
- Applicants Must Submit and Adequate Demonstration of Safety
- Review and Assessment of Safety Throughout the Life of the Facility
- Conduct Inspections of Facilities and Activities

8.7.2 Organization Related Principles

The design features relevant to the organization of the sociological portion of the environment are:

- Prime Responsibility for Nuclear Safety with Licensee
- Adequate Interfaces with Arrangements for Nuclear Security
- Enhance Safety Through International Cooperation
- Sufficient Number of Qualified Staff in Regulatory Body
- Independent Regulatory Body

8.7.3 Governance Related Principles

The design features relevant to the governance of the sociological portion of the environment are:

- Policy and Strategy for Nuclear Safety
- Governmental, Legal and Regulatory Framework
- Regulatory Requirements on Emergency Preparedness
- Provisions to deal with:
    - Accidents from Unregulated Sources
    - Safe Decommissioning
    - Building and Maintaining Competencies of all Parties

    - Technical Services
- Graded Approach to Regulation based on Radiation Risk
- Establishment of an Enforcement Policy for Non-compliances
- Establish Regulations and Guides

9 WEAKNESSES IN CURRENT NUCLEAR PRACTICE

9.1 Introduction

The purpose of this chapter is to identify weaknesses in nuclear industry current practice with the intent of later assessing whether the SEE approach can overcome these weaknesses in Chapter 12.

The accident that occurred in March 2011 at the Fukushima Daiichi nuclear power plant in Japan is used to identify weaknesses in current practices in the nuclear industry. Clearly the underlying causes of the accident in Japan will not be common to all nuclear power plant. Since the Fukushima accident is one of the worst nuclear accidents, the set of underlying causes represent a worst case against which to compare the SEE approach.

This section presents an overview of the accident (section 9.2) and then summarizes some of the key recommendations that were made from the many industry reports that analyzed the accident (section 9.3). The recommendations represent areas where the current practices at the Fukushima were inadequate.

9.2 Overview of the Accident[7]

This section outlines the events that lead to the accident so that the recommendations from the various industry reports can be better understood.

On March 11, 2011 a magnitude 9.0 earthquake, followed by a devastating series of tsunamis, struck off the northeastern coast of Japan approximately 175 km from the Fukushima Daiichi plant. The earthquake and tsunamis left an estimated 15,000 people dead, 2,500 people missing, about half a million homes destroyed or damaged, and 560 square kilometres of land inundated.

The combined impact of the earthquake and tsunamis on the Fukushima Daiichi nuclear power plant (NPP) caused one of the world's worst-ever nuclear

[7] The following overview of the accident is based on the reference documents listed in section 9.3 below.

accidents. In the hours and days that followed, the cores of three of the six reactors at the site melted down and released radioactive material over the surrounding region and to the sea. Radionuclides were released from the plant to the atmosphere and were deposited on land and on the ocean.

People within a radius of 20 km of the site and in other designated areas were evacuated, and those within a radius of 20–30 km were instructed to shelter before later being advised to voluntarily evacuate. Restrictions were placed on the distribution and consumption of food and the consumption of drinking water.

Earthquake

The earthquake caused a maximum ground acceleration of 0.56g at the power plant that was 25% greater than what plant was designed to withstand. At the time of the earthquake, Units 1, 2 and 3 were at full power. Units 4, 5 and 6 were shutdown for maintenance. Units 1 to 4 suffered serious damage from the earthquake. Units 1, 2 and 3 automatically shutdown, as designed.

As a result of the earthquake, offsite power was lost. The on-site replacement power facilities — emergency diesel generators — which were designed to deal with such loss of off-site power situations, automatically started in order to restore AC power in all six units.

Tsunamis

41 minutes after the earthquake a series of tsunami waves hit the plant. The height of the largest tsunami was approximately 15 meters. The original station design assumed a maximum tsunami height of 3.1 m, and was later updated to 5.6 m. Within 54 minutes after the earthquake the tsunamis stopped all emergency diesel generators and flooded the electrical switchgear. Units 1 to 4 were left with only battery power.

Reactor Cooling

Even when shutdown, a nuclear reactor needs to be cooled due to decay heat. Units 2 and 3 had steam driven pumps and so were able to maintain some cooling

for a few hours until the batteries drained. Unit 1 was the oldest unit and did not have steam driven pumps and hence it started overheating immediately.

Overpressure

Figure 46 shows the general arrangement of each of the reactors at the Fukushima Daiichi NPP.

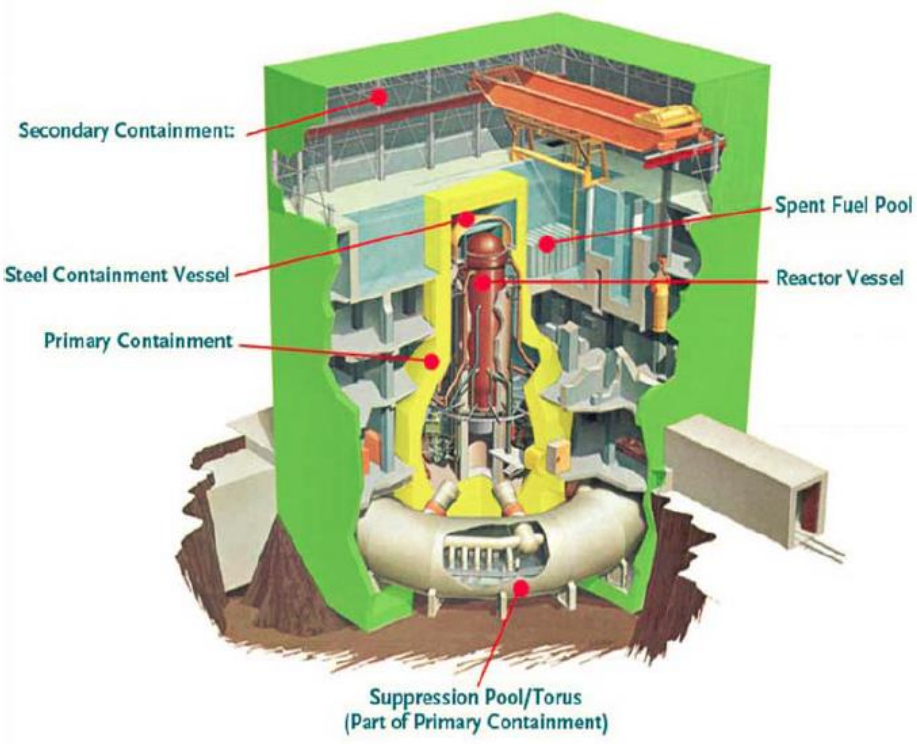


Figure 46 - General Arrangement of a Fukushima Reactor [47]

As the temperature in the reactors went up, so did the pressure. Operators had to vent some steam to the suppression pool in the primary containment to reduce the pressure. Since steam was being vented, eventually the reactor began to boil dry. As the core became uncovered it rapidly overheated, melting the fuel bundles. This produced hydrogen gas. The primary containment, where the suppression pool is located, is filled with nitrogen so that the hydrogen that was vented would not explode (due to lack of oxygen).

Since there was no functioning cooling system for the suppression pool it started to overheat, building up pressure in the primary containment. Operators had to vent primary containment to secondary containment to avoid primary containment failure. The hydrogen mixed with air in the secondary containment building

leading to an explosion that damaged the secondary containment building and possibly other equipment.

48 hours after the earthquake the main control room had to be evacuated due to high radiation readings.

Long Period Of Gradual Recovery

Over the next days, electrical and water supplies were slowly restored. High radiation levels and widespread damage impeded the recovery work. Venting of gases continued periodically to prevent over pressurization of containment. Highly radioactive water that had accumulated in low lying areas was discharged into the Pacific Ocean.

Offsite consequences

Significant releases of radioactive material to the atmosphere began when the reactor containments were vented, beginning at about 20 hours after the earthquake for unit 1 and over 40 hours after the earthquake for units 2 and 3. An evacuation zone of 20 km had already been established. The evacuation zone was later expanded to 30 km. With the evacuation zones in place, it seems unlikely that members of the public were exposed to external doses greater than 20 mSv/year. Although for radiation protection purposes it is assumed that all radiation exposures present a health risk, in practice, no adverse health effects have been observed at doses below about 100 mSv. Monitoring and control of food and water supplies were established over a wide area.

Summary of Key Issues

Figure 47 shows some of the key issues that were identified by the various investigation reports. Figure 48 shows some of the key causes of loss of critical safety related functionality during the Fukushima accident.

The fundamental issue was that the design basis of the plant did not adequately take into account the maximum size of an earthquake and resulting tsunami. Significantly, this resulted in failings of most of the layers of the defence in depth strategy that was used to achieve the plant's safety goals.

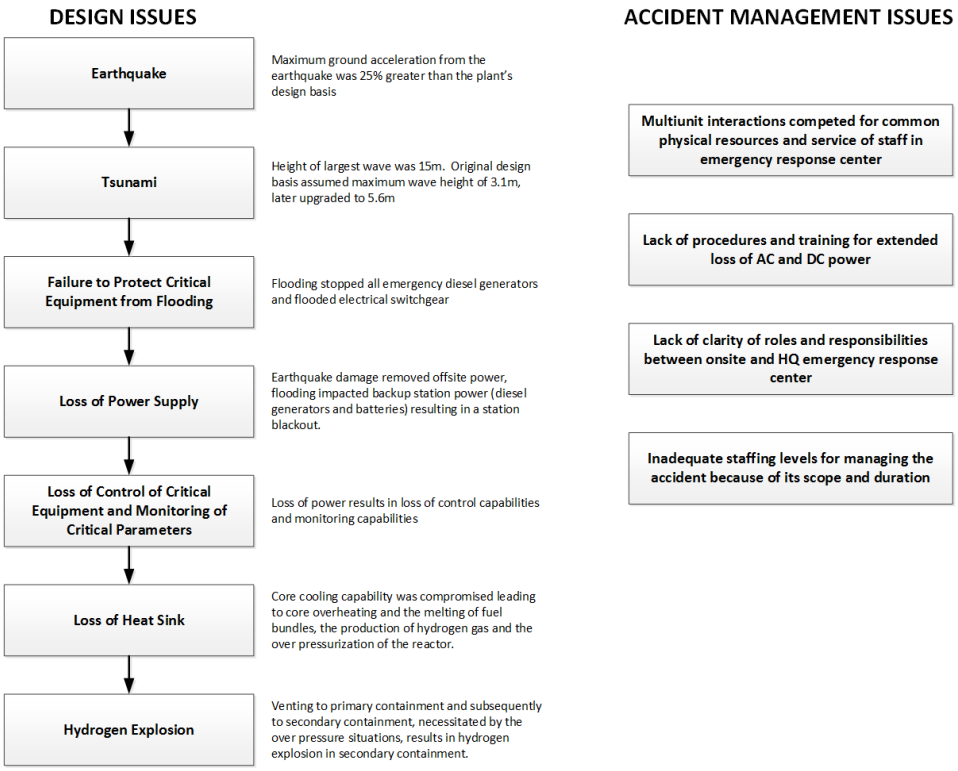


Figure 47 - Issues Associated with Fukushima Accident

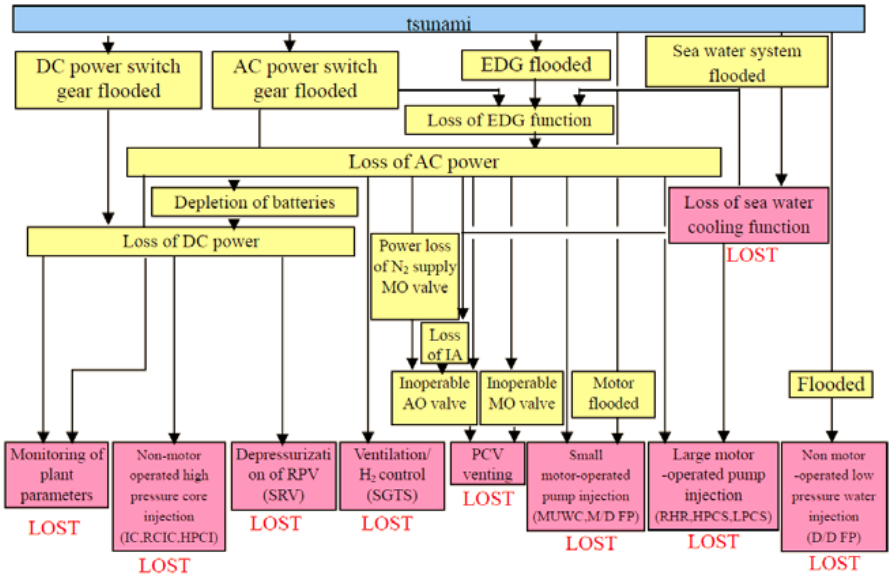


Figure 48 - Causes of Loss of Critical Functions at Fukushima [48]

9.3 Recommendations from Investigations

This section summarizes recommendations from eight reports that investigated the accident at the Fukushima Daiichi plant. These recommendations are used to assess the effectiveness of the SEE approach by assessing the degree to which application of the SEE approach would address the recommendations (see Chapter 12).

The recommendations are also used as the basis of assessing whether compliance with the IAEA best practice principles (in Chapter 8) would have been sufficient to avoid the accident.

In order to understand the causes of the accident and determine changes necessary to avoid re-occurrence, both in Japan and in any nuclear power plant around the world, a number of investigations were launched. The summary in this Section is based on the following publicly available reports.

Japanese Reports

1) Fukushima Nuclear Accident Analysis Report (TEPCO – owner of Fukushima Daiichi NPP) [48]
2) Report of the Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations (Japanese Government) [49]
3) Examination of Accident at Tokyo Electric Power Co., Inc.'s Fukushima Daiichi Nuclear Power Station and Proposal of Countermeasures. (Japan Nuclear Technology Institute) [50]
4) Executive Summary of the Final Report (Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company) [51]

Nuclear Industry Organizations

5) The Fukushima Daiichi Accident (IAEA) [52]
6) Lessons Learned from the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station (INPO) [53]

Nuclear Regulators

7) CNSC Fukushima Task Force Report (CNSC) [47]

8) Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants (US NRC) [1]

These reports both document the accident and provide an analysis of the underlying causes for the accident. The analyses provide the basis for a number of lessons learned from the accident that are being used by the international nuclear community to assess their current designs and practices.

The recommendations for changes to address the underlying causes of the accident, as documented in the above reports, are listed in Appendix 4. Each recommendation is categorized as to whether it reflects an aspect that should have been addressed in either the Design and Construction phase of the plant, or the Operations and Maintenance phase. Each recommendation is further categorized as to whether it impacts the physical plant, business processes, organization or governance within that phase. This facilitates the assessment of whether the principles in Appendix 3 provide adequate guidance relative to each recommendation. The principles that provide guidance are listed, and if there were no relevant principles for a recommendation then "None" was listed in the Principles column.

Each of the above reports is organized differently and hence groups its recommendations differently. The most comprehensive report was the report from the IAEA which was issued in 2015 which was after all the other reports were issued. It therefore benefited from having the results from the other reports available as input. The IAEA report is the result of an extensive international collaborative effort involving five working groups with about 180 experts from 42 Member States (with and without nuclear power programmes) and several international bodies. The report consists of a summary report (222 pages) and five technical volumes (over 1100 pages total). The recommendations from the IAEA report are used to represent the results from all the reports in assessing the degree to which the SEE approach addresses these recommendations (see Chapter 12).

The seventeen major recommendations (as described below) made in the IAEA report are used to represent all the detailed recommendations from the other seven reports.

A major factor that contributed to the accident was the widespread assumption in Japan that its nuclear power plants were so safe that an accident of this magnitude was simply unthinkable. This assumption was accepted by nuclear power plant

operators and was not challenged by regulators or by the Government. As a result, Japan was not sufficiently prepared for a severe nuclear accident in March 2011.

"Design basis accidents are accidents against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits. Beyond design basis accidents are accident conditions more severe than a design basis accident." [22] The size of the earthquake and the subsequent size of tsunami were beyond the size that was assumed by the design basis. The Fukushima accident was therefore a beyond design basis accident. Figure 49 shows the impact of the insufficient consideration of this beyond design basis accident.

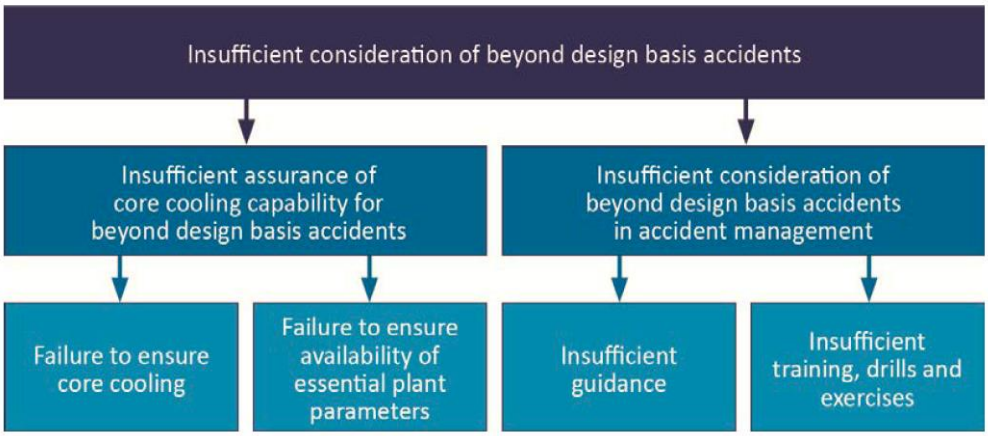


Figure 49 - Impact of the insufficient consideration of beyond design basis accidents [52]

In the IAEA report, the lessons learned are grouped by:

- Nuclear Safety Considerations
- Emergency Preparedness and Response
- Radiological Consequences, and
- Post-Accident Recovery

Each of these groups of recommendations are summarized below. The full list of recommendations from all eight reports are in Appendix 4.

Section 9.3.5 summarizes some key findings from the US NRC report [1] that are relevant to this thesis since they identify areas for improvement to the regulation of nuclear plant safety.

9.3.1 IAEA - Nuclear Safety Considerations

The nuclear safety related recommendations were:

1. The assessment of natural hazards needs to be sufficiently conservative

2. The safety of NPPs needs to be re-evaluated on a periodic basis to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly

3. The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on an NPP. The assessment of natural hazards also needs to consider their effects on multiple units at an NPP.

4. Operating experience programmes need to include experience from both national and international sources. Safety improvements identified through operating experience programmes need to be implemented promptly. The use of operating experience needs to be evaluated periodically and independently.

5. The defence in depth concept remains valid, but implementation of the concept needs to be strengthened at all levels by adequate independence, redundancy, diversity and protection against internal and external hazards. There is a need to focus not only on accident prevention, but also on improving mitigation measures.

6. Instrumentation and control systems that are necessary during beyond design basis accidents need to remain operable in order to monitor essential plant safety parameters and to facilitate plant operations.

7. Robust and reliable cooling systems that can function for both design basis and beyond design basis conditions need to be provided for the removal of

residual heat.

8. There is a need to ensure a reliable confinement function for beyond design basis accidents to prevent significant release of radioactive material to the environment.

9. Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a plant to withstand applicable beyond design basis accidents and to provide a high degree of confidence in the robustness of the plant design.

10. Accident management provisions need to be comprehensive, well designed and up to date. They need to be derived on the basis of a comprehensive set of initiating events and plant conditions and also need to provide for accidents that affect several units at a multi-unit plant.

11. Training, exercises and drills need to include postulated severe accident conditions to ensure that operators are as well prepared as possible. They need to include the simulated use of actual equipment that would be deployed in the management of a severe accident.

12. In order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body is independent and possesses legal authority, technical competence and a strong safety culture.

13. In order to promote and strengthen safety culture, individuals and organizations need to continuously challenge or re-examine the prevailing assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety.

14. A systemic approach to safety needs to consider the interactions between human, organizational and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations.

9.3.2 IAEA - Emergency Preparedness and Response

The recommendations in the area of emergency preparedness and response include recommendations:

- To consider emergencies that could include severe damage to the fuel including to several units at a multi-unit plant,
- To clearly define roles and responsibilities for the operating organization, and for local and national authorities,
- To assign emergency workers clear duties, provide adequate training and provide proper protection during an emergency,
- To improve decision making during emergencies by establishing predetermined actions based on plant conditions, and making arrangements for enabling protective actions to be extended or modified in response to developing plant conditions, and
- To make arrangements for notification, assistance and consultation among States.

9.3.3 IAEA - Radiological Consequences

The recommendations in the area of radiological consequences include recommendations:

- To establish a comprehensive and coordinated program of long term environmental monitoring, in case of an accidental release of radioactive substances,
- To develop, with relevant international bodies, explanations of the principles and criteria for radiation protection that are understandable by a non-specialist,
- To establish consistency between international standards and national standards activity concentrations associated with drinking water, food and non-edible consumer products,
- To establish a robust system for monitoring and recording radiation doses that may be incurred by workers during severe accident management activities,

- To establish radiological protection guidance to address psychological consequences to members of the affected population in the aftermath of radiological accidents, and
- To establish an integrated perspective to ensure sustainability of agriculture, forestry, fishery and tourism following a large release of radionuclides.

9.3.4 IAEA - Post-Accident Recovery

The recommendations in the area of radiological consequences include recommendations:

- To establish pre-accident plans for post-accident recovery to improve decision making under pressure in the immediate post-accident situation,
- To establish remediation strategies that take into account the effectiveness and feasibility of individual measures,
- To establish further international guidance on the practical application of safety standards for radiation protection in post-accident recovery situations,
- To establish a strategic plan for maintaining long term stable conditions and for the decommissioning of accident damaged facilities, and
- To establish a national strategy for post-accident recovery.

9.3.5 US NRC - Key Findings [1]

There were some key findings from the US NRC report that are important for the hypothesis of this thesis since they speak to the need for improvement to the regulation of nuclear plant safety.

One key observation was that “Four decades of analysis and operating experience have demonstrated that nuclear plant core-damage risks are dominated by beyond-design-basis accidents. Such accidents can arise, for example, from multiple human and equipment failures, violations of operational protocols, and extreme external events.”

This observation aligns with Leveson's observation in [2] that "While the traditional approaches worked well for the simpler systems of the past for which they were devised, significant changes have occurred in the types of systems". Leveson identifies the following factors that contribute to traditional safety engineering's inability to adequately handle complex systems:

- Fast pace of technological change
- Reduced ability to learn from experience
- Changing Nature of Accidents
- New types of hazards
- Increasing complexity and coupling
- Decreasing tolerance for single accidents
- Difficulty in selecting priorities and making trade-offs
- More complex relationships between humans and automation, and
- Changing regulatory and public views of safety

Leveson's observation aligns with the finding from the US NRC report which concludes that "Current approaches for regulating nuclear plant safety, which traditionally have been based on deterministic concepts such as the design-basis accident, are clearly inadequate for preventing core-melt accidents and mitigating their consequences. Modern risk assessment principles are beginning to be applied in nuclear reactor licensing and regulation. The more complete application of these principles in licensing and regulation could help to further reduce core-melt risks and their consequences and enhance the overall safety of all nuclear plants, especially currently operating plants."

The SEE approach is an example of a more modern approach that can better address beyond design basis accidents.

10 WEAKNESSES IN NUCLEAR BEST PRACTICE

10.1 Introduction

The purpose of this chapter is to identify weaknesses in nuclear industry best practice with the intent of later assessing whether the SEE approach can overcome these weaknesses in Chapter 12.

Chapter 9 identified recommendations from industry analysis of the Fukushima accident that indicate weaknesses in the 2011 current practices at TEPCO, the utility responsible for Fukushima, that lead to the accident. This chapter compares these recommendations to the IAEA best practices principles identified in Chapter 8 to assess whether there are best practice principles to address each of the recommendations.

Appendix 4 shows either a non-compliance with best practice principles by TEPCO, or a gap in the best practice principles due to a lack of principles to address the Fukushima recommendations. Recommendations for which there are not adequate principles represent areas of weakness in the best practice principles.

An assessment was also done to assess the changes to IAEA best practice documents that resulted from analyses of the Fukushima accident to determine if the changes were sufficient to address the identified areas of weaknesses in current practice at Fukushima.

The overall process is represented diagrammatically in Figure 50.

The remaining sections of this chapter present:

- An assessment of the adequacy of the changes made to best practice documents to address the Fukushima recommendations (section 10.2)
- An assessment of which recommendations are adequately covered by IAEA principles, (section 10.3) and
- An assessment of which recommendations were not adequately covered by the best practice principles and hence indicate gaps in the principles (section 10.4)

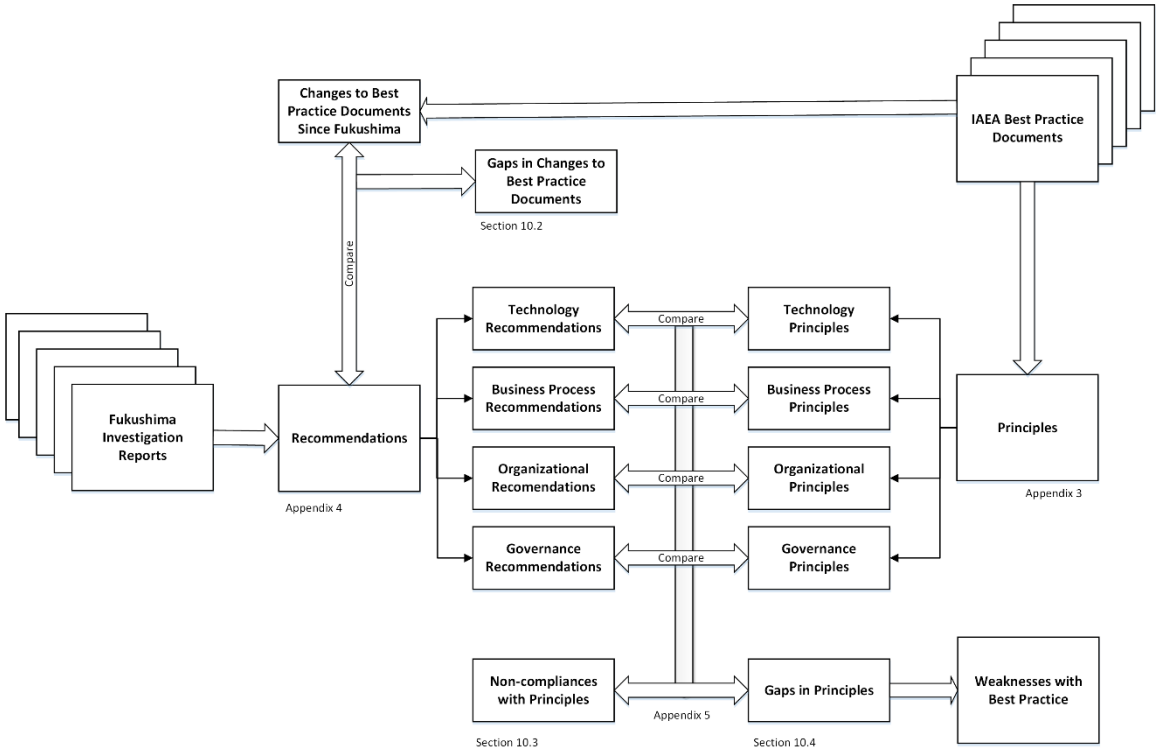


Figure 50 - Assessment of Weaknesses in Nuclear Best Practice

10.2 Gaps in Updates to Best Practice Principles

Two key IAEA best practice documents were updated as a result of the Fukushima accident:

1. International Atomic Energy Agency. 2016. *Safety of Nuclear Power Plants: Design.* [31]
2. International Atomic Energy Agency. 2016. *Safety of Nuclear Power Plants: Commissioning and Operation* [32]

Figure 51 shows the main areas that were revised in each document and which requirements were updated in those areas.

Changes were made in the following areas:

- Prevention of severe accidents by strengthening the design basis for the plant,
- Prevention of unacceptable radiological consequences of a severe accident for the public and the environment,
- Mitigation of the consequences of a severe accident to avoid or to minimize radioactive contamination off the site,
- Periodic safety review and feedback from operating experience,
- Emergency preparedness,
- Accident management, and
- Fire safety.

Appendix 5 shows the specific changes that were made to each requirement in these areas.

Each of the seventeen recommendations for improvement identified in section 9.3 were assessed to determine if the changes in Appendix 5 were adequate to address the recommendation. The following recommendations were found to not have adequate changes to requirements necessary to address the recommendation:

- The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on an NPP. The assessment of natural hazards also needs to consider their effects on multiple units at an NPP.
- Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a plant to withstand applicable beyond design basis accidents and to provide a high degree of confidence in the robustness of the plant design.
- In order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body is independent and possesses legal authority, technical competence and a strong safety culture.
- In order to promote and strengthen safety culture, individuals and organizations need to continuously challenge or re-examine the prevailing assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety.
- A systemic approach to safety needs to consider the interactions between human, organizational and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations.
- Planning for post-accident recovery needs to be implemented

Figure 51 - Changes to IAEA Best Practice Documents Since Fukushima [47] [48]

10.3 Non-compliances with Best Practice Principles

Some of the recommendations from the Fukushima reports were a result of TEPCO's non-compliance with industry best practice as documented in IAEA documents. Appendix 4 lists 206 recommendations from the eight reference reports[8]. For each of the recommendations, principles from Appendix 3 (IAEA Best Practice Principles) were identified that, if applied, would have avoided the need for making the recommendation.

Recommendations for which one or more principles were identified indicate areas where TEPCO was non-compliant with IAEA guidance. Recommendations for which no principles were identified indicate areas where IAEA guidance is lacking. The gaps in IAEA principles are discussed in section 10.4.

Table 5 shows which IAEA document contained principles that were associated with recommendations and the number of principles from each document. This gives an indication of which IAEA documents were the largest source of non-compliance by TEPCO.

IAEA Document	Number of Principles Associated with Recommendations
Safety of Nuclear Power Plants: Design. [31]	4
Safety of Nuclear Power Plants: Commissioning and Operation [32]	8
Leadership and Management for Safety [46]	4
Governmental, Legal and Regulatory Framework for Safety [54]	15
Fundamental Safety Principles. [43]	8
Basic Safety Principles for Nuclear Power Plants [44]	37

[8] There were not 206 distinct recommendations since similar recommendations were made by more than one report.

Defence in Depth in Nuclear Safety: A Report [45]	2

Table 5 - Number of Principles Associated with Recommendations

The principles in Table 5 cover design margins, safety culture, regulatory oversight and emergency preparedness.

10.4 Gaps in Best Practice Principles

The 129 recommendations in Appendix 4 that did not have principles associated with them cover seventeen summary recommendations made in the IAEA report [52] that was issued well after all the other reports reviewed in section 9.3. Later in the thesis the seventeen summary recommendations are used to assess the SEE approach in order to deal with a more manageable number of recommendations.

The seventeen summary recommendations and the number of detailed recommendations in Appendix 4 that they cover are:

1. The assessment of natural hazards needs to be sufficiently conservative (2 detailed recommendations)
2. The safety of NPPs needs to be re-evaluated on a periodic basis to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly (2 detailed recommendations)
3. The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on an NPP. The assessment of natural hazards also needs to consider their effects on multiple units at an NPP. (5 detailed recommendations)
4. Operating experience programmes need to include experience from both national and international sources. Safety improvements identified through operating experience programmes need to be implemented promptly. The use of operating experience needs to be evaluated periodically and independently. (3 detailed recommendations)
5. The defence in depth concept remains valid, but implementation of the concept needs to be strengthened at all levels by adequate independence, redundancy, diversity and protection against internal and external hazards.

There is a need to focus not only on accident prevention, but also on improving mitigation measures. (17 detailed recommendations)

6. Instrumentation and control systems that are necessary during beyond design basis accidents need to remain operable in order to monitor essential plant safety parameters and to facilitate plant operations. (4 detailed recommendations)
7. Robust and reliable cooling systems that can function for both design basis and beyond design basis conditions need to be provided for the removal of residual heat. (4 detailed recommendations)
8. There is a need to ensure a reliable confinement function for beyond design basis accidents to prevent significant release of radioactive material to the environment. (5 detailed recommendations)
9. Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a plant to withstand applicable beyond design basis accidents and to provide a high degree of confidence in the robustness of the plant design. (2 detailed recommendations)
10. Accident management provisions need to be comprehensive, well designed and up to date. They need to be derived on the basis of a comprehensive set of initiating events and plant conditions and also need to provide for accidents that affect several units at a multi-unit plant. (3 detailed recommendations)
11. Training, exercises and drills need to include postulated severe accident conditions to ensure that operators are as well prepared as possible. They need to include the simulated use of actual equipment that would be deployed in the management of a severe accident. (4 detailed recommendations)
12. In order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body is independent and possesses legal authority, technical competence and a strong safety culture. (5 detailed recommendations)
13. In order to promote and strengthen safety culture, individuals and organizations need to continuously challenge or re-examine the prevailing assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety. (2 detailed recommendations)
14. A systemic approach to safety needs to consider the interactions between human, organizational and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations. (2 detailed recommendations)

15. Emergency preparedness and response needs to be strengthened (46 detailed recommendations)
16. Improve monitoring and management of radiological consequences (17 detailed recommendations)
17. Planning for post-accident recovery needs to be implemented (6 detailed recommendations)

Nuclear Safety Considerations Recommendations

In this area the recommendations that were not adequately covered by IAEA principles focus mainly on dealing with low probability, high consequence accidents (beyond design basis accidents). The recommendations address risk management taking into account uncertainties, complexities and interactions between systems, units and the environment. The adequacy of the safety culture, both within the utility and the regulator, is a common theme in all areas.

Emergency Preparedness and Response Recommendations

In this area the recommendations that were not adequately covered by IAEA principles focused mainly on issues of staffing, training and the adequacy of procedures to deal with a large scope accident as was experienced at the Fukushima plant.

Radiological Consequences Recommendations

In this area the recommendations that were not adequately covered by IAEA principles focused mainly on means to assess exposures by staff and the public, and the means to effectively communicate with the public.

Post-Accident Recovery Recommendations

In this area the recommendations that were not adequately covered by IAEA principles focused mainly on the adequacy of pre-accident planning for recovery and the ability to manage the socioeconomic impacts of a large scale accident.

The 129 recommendations that did not have principles associated with them can also be viewed from the perspective of which lifecycle phase had a failing that led to the recommendation and whether the failing was of a business process, the organization or the governance. The following Sections summarize some of the failings in each of these areas.

Design & Construction – Business Processes Failings

Inadequate consideration of beyond-design-basis accidents

- Multiple human and equipment failures
- Violation of operational protocols
- Extreme external events

Operations & Maintenance – Business Processes Failings

- Inadequate assessment of combinations of events including impacts on multi-unit stations
- Corporate risk management process did not consider low-probability, high-consequence events
- Inadequate preparedness for retrieving and removing damaged fuel
- Inadequate procedures for venting containment
- Inadequate emergency response plans with respect to support for operator actions
- Inadequate off-site emergency management capability for extreme events affecting a large region
- Lack of strategies to manage contaminated liquid and solid waste
- Inadequate procedures with respect to taking into account the impact of accidents on staff's ability to respond and take actions
- Inadequate control of emergency supplies
- Inadequate processes for establishing a recovery program after the accident
- Lack of strategies to minimize ingestion doses from food sources

- Estimation of radiation doses did not take into account personal radiation monitoring of representative groups of the public
- Lack of strategies to mitigate psychological consequences of accidents

Operations & Maintenance – Organization Failings

- Inadequate strategies for staffing emergency response organization quickly and over a long duration accident
- Inadequate staffing for nuclear safety and emergency response functions
- Inadequate training to respond to severe accidents
- Inadequate accident response environment
- Inadequate means for monitoring critical plant parameters and providing emergency response functions (including lack of training in the means)
- Inadequate procedures, equipment and staffing to support emergency response actions
- Inadequate definition of roles and responsibilities to support post-accident communication and decision making

Operations & Maintenance – Governance Failings

- Inadequate arrangements to ensure decisions balance good vs harm
- Lack of alignment of decision criteria for consumer products to be compliant with international standards
- Ineffective communication of risks to the public
- Ineffective use of health surveys after the accident
- Inadequate pre-accident planning for post-accident recovery
- Inadequate remediation strategies
- Lack of guidance on application of safety standards in post-accident recovery situations
- Lack of plans for socio-economic revitalization and reconstruction after a major accident
- Inadequate plans, training and guidance to deal with emotional impacts

11 SAFETY ENTERPRISE ENGINEERING EXAMPLE

11.1 Approach

The hypothesis of this thesis is that:

> "safety goals can be more effectively achieved by applying an engineering approach to the design, operation, maintenance and evolution of the enterprise and the technologies for which it is responsible that integrates applicable principles and practices from safety engineering, systems engineering, management science and enterprise architecture".

Previous Chapters of the thesis have outlined the Safety Enterprise Engineering (SEE) approach by defining:

Safety Enterprise Engineering Process (Chapter 5),

Hazard Analysis of Socio-technical Systems (Chapter 6),

Models of the Enterprise (Chapter 7) and

Nuclear Best Practices Applicable to Various Views of the Enterprise Architecture: technology, business process, organization and governance views (Chapter 8).

This Chapter presents an example of the application of the SEE approach to a typical nuclear power utility. In Chapter 12 the example is assessed to determine the degree to which the approach addresses weaknesses in current and best nuclear industry practice described in Chapters 9 and 10.

The SEE approach was applied to a slice of safety related functionality of a typical CANDU power utility. A CANDU power utility was chosen due to the author's familiarity with CANDU utilities and power plants, and because detailed information about the Fukushima plant and the business processes, organization and governance of the TEPCO utility, that was responsible for the plant, was not readily available.

Figure 52 shows these various elements of the example graphically. The diagram shows the content of various Chapters of the thesis (both inside this Chapter and outside the Chapter) that were used to reach the conclusions in Chapter 12). The arrows in the diagram indicate information used to develop the content of each section.

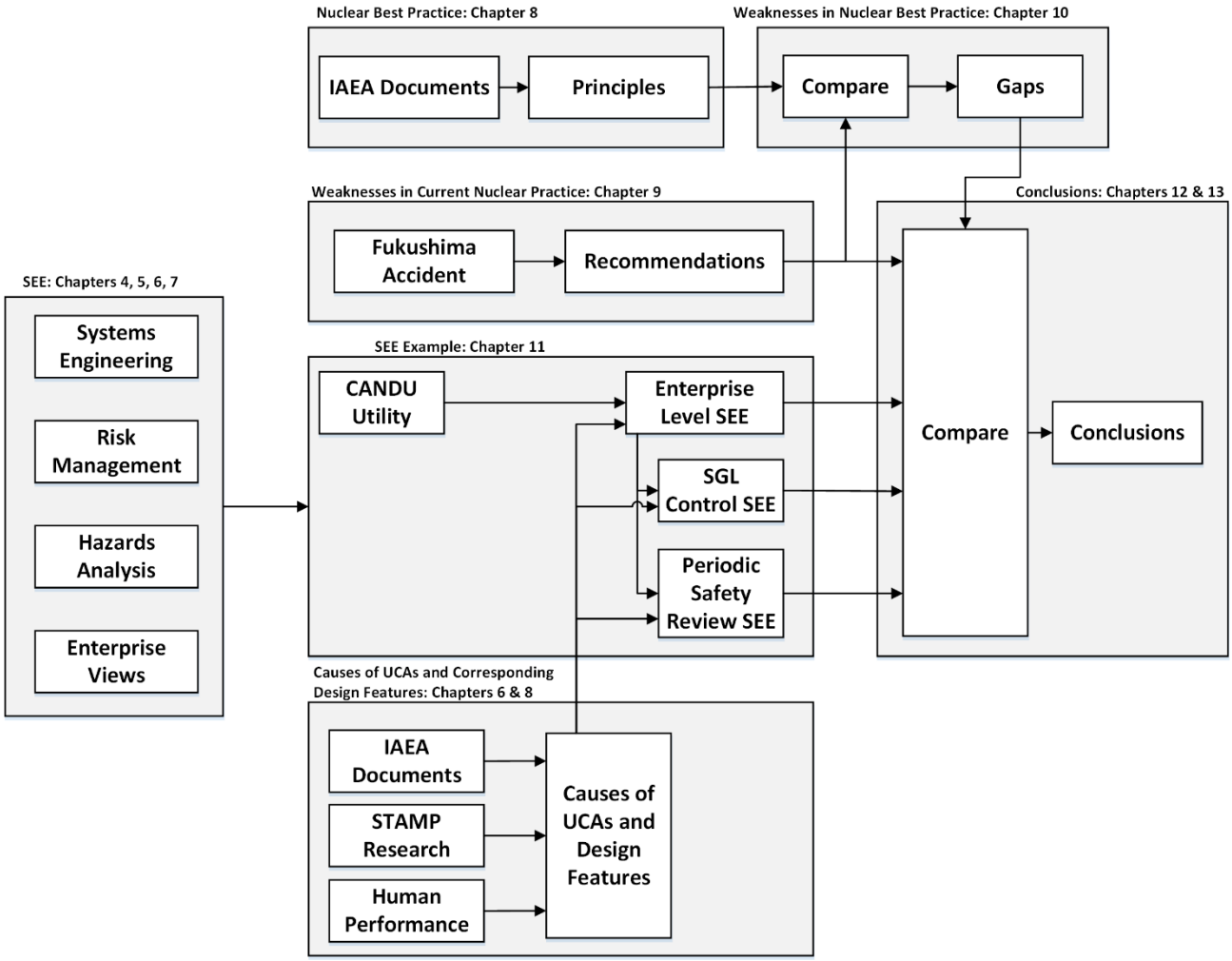


Figure 52 - Elements of the Example

11.2 SEE Approach Applied to a Typical CANDU Utility

This section applies the Safety Enterprise Engineering approach to a typical utility responsible for a CANDU nuclear power plant to assess the effectiveness of the approach at addressing some of the underlying causes of the Fukushima accident.

To avoid having to engineer the full scope of safety functionality of a nuclear utility, the example will be limited to the engineering of the utility at a high-level of abstraction and then the drilldown to the engineering of two slices of safety related functionality; a technology based slice (steam generator level control) and a non-technology slice (the periodic safety review process).

Even though the example is limited in scope, it provides a basis to demonstrate the effectiveness of the SEE approach in many areas where weaknesses in nuclear industry practice were identified.

11.2.1 Overview

The following Sections document the application of the SEE approach to a slice of safety related functionality of a typical CANDU utility:

- Utility Level Engineering (Section 11.2.2)
  - Utility Level Safety Requirements
  - Utility Level – Technology View
    - Technology Safety Requirements
    - Technology Architecture
    - Technology Hazard analysis
  - Utility Level – Business Process View
    - Business Process Safety Requirements
    - Business Process Architecture
    - Business Process Hazard analysis
- Steam Generator Level Controls Engineering (Section 11.2.3)
  - Steam Generator Level Controls Safety Requirements
  - Steam Generator Level Controls Architecture
  - Steam Generator Level Controls Hazard analysis
- Periodic Safety Review (PSR) Process Engineering (Section 11.2.4)
  - PSR Process Safety Requirements
  - PSR Process Architecture
  - PSR Process Hazard analysis

Conclusions are then made with respect to the Safety Enterprise Engineering approach's ability to address the recommendations made from the analyses of the Fukushima accident (in Chapter 12).

11.2.2 Utility Level Engineering

At the utility level, the whole nuclear power utility (including the nuclear power stations that it operates) is treated as a system. As described in Section 5.1, a systems engineering process is applied to this system. The systems engineering process includes definition of the system safety requirements, definition of the architecture of the system and then the application of the safety engineering process, as described in Section 5.2, to manage the safety risks associated with the system.

Section 7.4 provides a partial model of a typical nuclear utility. In particular, it provides a model for the technology, business process, organizational, and governance views of the overall architecture of a nuclear utility.

These models will be used as the basis of the architecture of the utility and the basis of the safety engineering done at this level.

Since the example is limited in scope to the Steam Generator Level Controls and the Periodic Safety Review Process, at the Enterprise Level the example will be limited to the Technical View of the enterprise and the Business Process View of the enterprise.

Figure 53 and Figure 54 provide graphical representations of the steps taken in the engineering of the Technology View of the enterprise and the Business Process View of the enterprise respectively. The two figures show the main outcomes of each step in the SEE process.

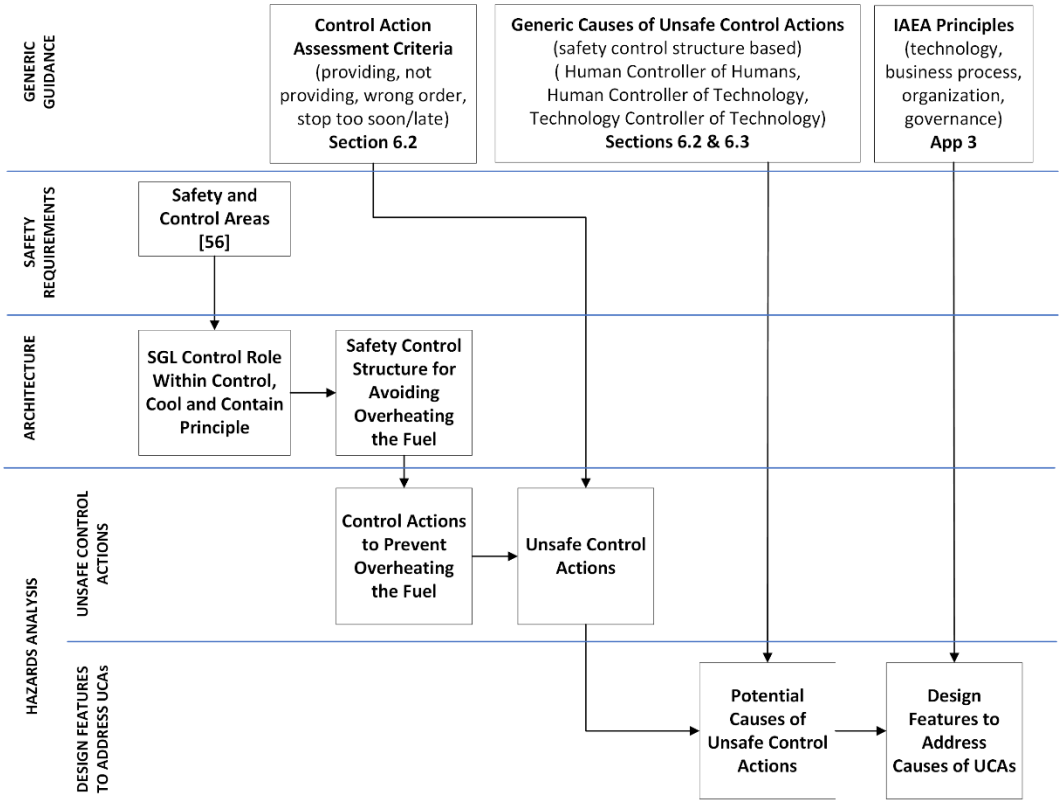


Figure 53 - Engineering of Utility - Technology View

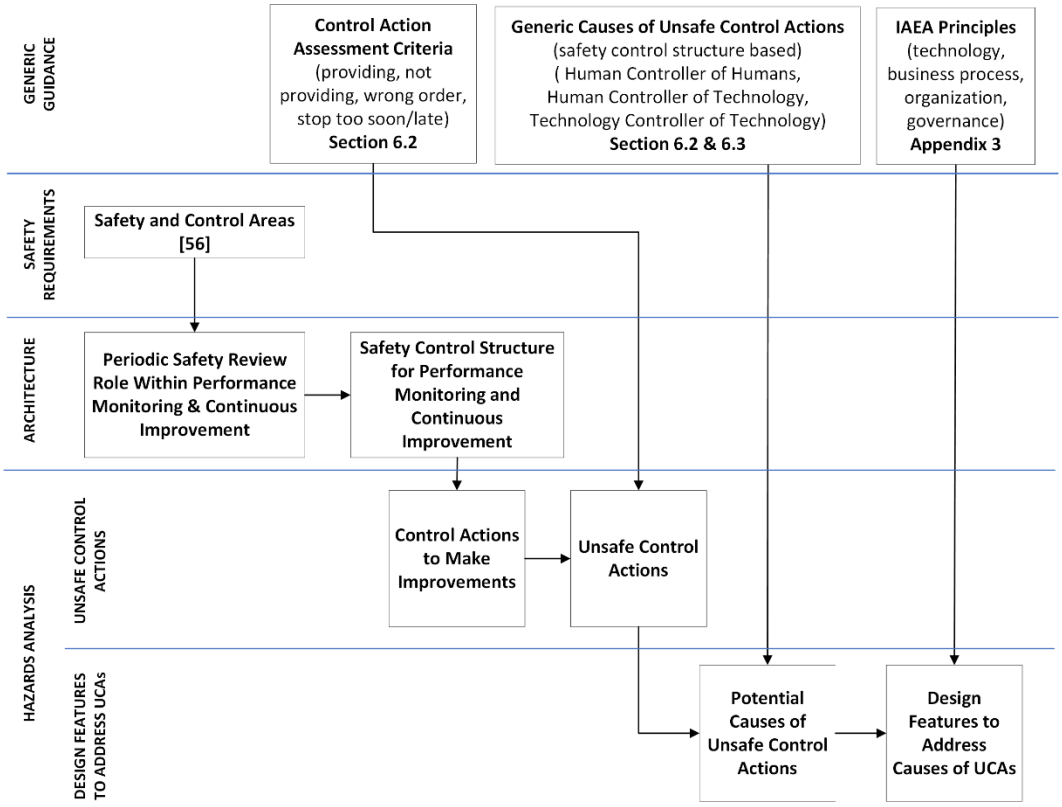


Figure 54 - Engineering of Utility - Business Process View

11.2.2.1 Utility Safety Requirements

Every country with a nuclear power program establishes a legal and regulatory framework that establishes expectations for the safe use of nuclear power. The IAEA has issued the following documents that provide expectations on this legal and regulatory framework:

- Establishing the safety infrastructure for a nuclear power programme [55]
- Governmental, legal and regulatory framework for safety [54]

The legal and regulatory framework in Canada is established by the Canadian Nuclear Safety Commission. It has organized the expectations for a nuclear power utility in Canada in a set of regulatory documents. The documents have been organized in a set of 14 Safety and Control Areas (SCAs) [56]. Table 6 lists the 14 safety and control areas and provides a description of each along with the regulatory documents that provide the detailed requirements in each area.

Safety & Control Area	**Description & Regulatory Documents**
Management System	The framework that establishes the processes and programs required to ensure an organization achieves its safety objectives, continuously monitors its performance against these objectives, and fosters a healthy safety culture. REGDOC 2.2.1 Management Systems REGDOC 2.1.2 Safety Culture
Human Performance Management	The activities that enable effective human performance through the development and implementation of processes that ensure a sufficient number of licensee personnel are in all relevant job areas and have the necessary knowledge, skills, procedures and tools in place to safely carry out their duties. REGDOC 2.2.1 Human Factors REGDOC 2.2.2 Personnel Training REGDOC 2.2.3 Personnel Certification REGDOC 2.2.4 Fitness for Duty
Operating Performance	This includes an overall review of the conduct of the licensed activities and the activities that enable effective performance. REGDOC 2.3.1 Conduct of Licensed Activities REGDOC 2.3.2 Accident Management REGDOC 2.3.3 Periodic Safety Review
Safety Analysis	Maintenance of the safety analysis that supports the overall safety case for the facility. Safety analysis is a systematic evaluation of the potential hazards associated with the conduct of a proposed activity or facility and considers the effectiveness of preventative measures and strategies in reducing the effects of such hazards. REGDOC 2.4.1 Deterministic Safety Analysis REGDOC 2.4.2 Probabilistic Safety Analysis REGDOC 2.4.3 Criticality Safety REGDOC 2.4.4 Safety Analysis for Class 1B Facilities

Safety & Control Area	**Description & Regulatory Documents**
Physical Design	The activities that impact the ability of structures, systems and components to meet and maintain their design basis given new information arising over time and taking changes in the external environment into account REGDOC 2.5.1, General Design Considerations REGDOC 2.5.2, Design of Reactor Facilities: Nuclear Power Plants REGDOC 2.5.3, Design of Reactor Facilities: Small Reactors REGDOC 2.5.4, Design of Uranium Mines and Mills REGDOC 2.5.5, Design of Fixed Radiography Installations REGDOC 2.5.6, Design of Nuclear Substance Laboratories and Nuclear Medicine Rooms REGDOC 2.5.7, Design of Exposure Devices
Fitness for Service	The activities that impact the physical condition of structures, systems and components to ensure that they remain effective over time. This area includes programs that ensure all equipment is available to perform its intended design function when called upon to do so. REGDOC 2.6.1, Equipment Fitness for Service and Equipment Performance REGDOC 2.6.2, Maintenance REGDOC 2.6.3, Aging Management
Radiation Protection	The implementation of a radiation protection program in accordance with the *Radiation Protection Regulations*. This program must ensure that contamination levels and radiation doses received by individuals are monitored and controlled, and maintained as low as reasonably achievable (ALARA) REGDOC 2.7.1 Radiation Protection REGDOC 2.7.2 Dosimetry
Conventional Health & Safety	The implementation of a program to manage workplace safety hazards and to protect personnel and equipment.
Environmental Protection	The programs that identify, control and monitor all releases of radioactive and hazardous substances and effects on the environment from facilities or as the result of licensed activities. REGDOC 2.9.1, Environmental Protection Environmental Principles, Assessments and Protection Measures

Safety & Control Area	Description & Regulatory Documents
Emergency Management & Fire Protection	The emergency plans and emergency preparedness programs which exist for emergencies and for non-routine conditions. This area also includes any results of participation in exercises. REGDOC 2.10.1, Nuclear Emergency Preparedness and Response REGDOC 2.10.2, Fire Protection
Waste Management	The internal waste-related programs that form part of the facility's operations up to the point where the waste is removed from the facility to a separate waste management facility. This area also covers the planning for decommissioning. REGDOC 2.11.1, Waste Programs REGDOC 2.11.2, Decommissioning Planning
Security	The programs required to implement and support the security requirements stipulated in the regulations, in the license, in orders, or in expectations for the facility or activity. REGDOC 2.12.1, High Security Facilities (CONFIDENTIAL) REGDOC 2.12.2, Site Access Security Clearance REGDOC 2.12.3, Security of Nuclear Substances
Safeguards & Non-proliferation	The programs required for the successful implementation of the obligations arising from the Canada/IAEA safeguards agreements, as well as all other measures arising from the *Treaty on the Non-Proliferation of Nuclear Weapons.* REGDOC 2.13.1, Safeguards and Nuclear Material Accountancy REGDOC 2.13.2, Import and Export
Packaging & Transport	The programs that manage the safe packaging and transport of nuclear substances and radiation devices to and from the licensed facility. REGDOC 2.14.1, Packaging and Transport

Table 6 - CNSC Safety & Control Areas [57]

Satisfying the requirements reflected in the set of regulatory documents in the 14 safety and control areas has been established as satisfying the overall safety goal in Canada as reflected in the stated purpose of the Nuclear Safety Control Act [58]:

"The purpose of this Act is to provide for:

(a) the limitation, to a reasonable level and in a manner that is consistent with Canada's international obligations, of the risks to national security, the health and safety of persons and the environment that are associated with the development, production and use of nuclear energy and the production, possession and use of nuclear substances, prescribed equipment and prescribed information; and

(b) the implementation in Canada of measures to which Canada has agreed respecting international control of the development, production and use of nuclear energy, including the non-proliferation of nuclear weapons and nuclear explosive devices."

These requirements therefore are the safety requirements for a nuclear utility in Canada.

11.2.2.2 Utility Level – Technology View

This Section applies the SEE approach to the technology view of the enterprise. For the technology view of the enterprise the following steps are done (as represented in Figure 53):

- The safety requirements for the technology are established
- The architecture of the technology is defined
- A hazard analysis of the technology is performed

Note that in this thesis all three of these outcomes are limited in scope, as they focus on establishing the context for the engineering of the Steam Generator Level Controls in Section 11.2.3.

11.2.2.2.1 Technology Safety Requirements

As per Table 6, the applicable requirements for the technology architecture come primarily from "REGDOC 2.5.2, Design of Reactor Facilities: Nuclear Power Plants" [59]. It establishes the following two qualitative safety goals:

- Individual members of the public shall be provided a level of protection from the consequences of NPP operation, such that there is no significant additional risk to the life and health of individuals.

- Societal risks to life and health from NPP operation shall be comparable to or less than the risks of generating electricity by viable competing technologies, and shall not significantly add to other societal risks.

It also establishes three quantitative safety goals with respect to:

- core damage frequency,
- small release frequency, and
- large release frequency

11.2.2.2.2 Technology Architecture

The "technology" in this example is the physical, nuclear power plant. The technology architecture is therefore the architecture of the nuclear power plant. Figure 36 and Figure 37 show the overall architecture of a CANDU nuclear power plant and its basic control systems. Figure 17 shows the major systems in a CANDU nuclear power plant showing the flow of energy from the nuclear reactor to the steam generator to the turbines and finally the generator. Figure 18 shows the major control systems involved in controlling these major systems.

In this example, two slices of safety related functionality will be analyzed in detail to demonstrate the Safety Enterprise Engineering approach. The first slice is the steam generator level controls (a technology related slice), and the second slice is the periodic safety review process (a business process slice).

As described in Section 8.3, one of the key design approaches used in this architecture to achieve the above safety goals is the concept of "defense in depth" [45].

Generally, there are only two ways in which radioactive material comes to be released. One way is through mechanical damage (for example due to earthquakes, or damage during refuelling) or the second way is caused by the fuel overheating and melting.

One of the key design principles within the defense in depth approach to deal with the risk of fuel overheating is to achieve "control, cool and contain" safety functions with a high degree of confidence. Figure 55 and Figure 56 illustrates the safety functions necessary to achieve "control, cool and contain" and how they relate to the steam generator level control system.

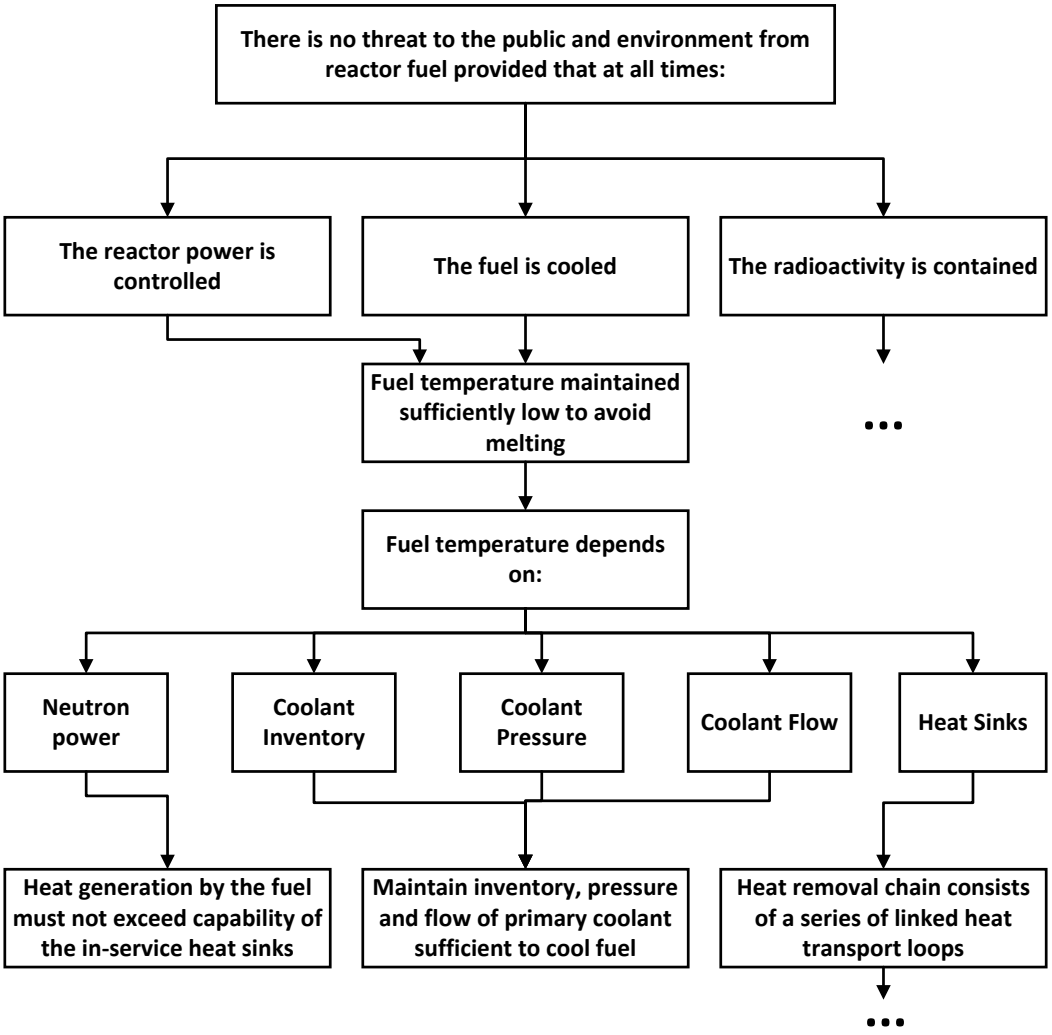


Figure 55 - Control, Cool and Contain Principle [39]

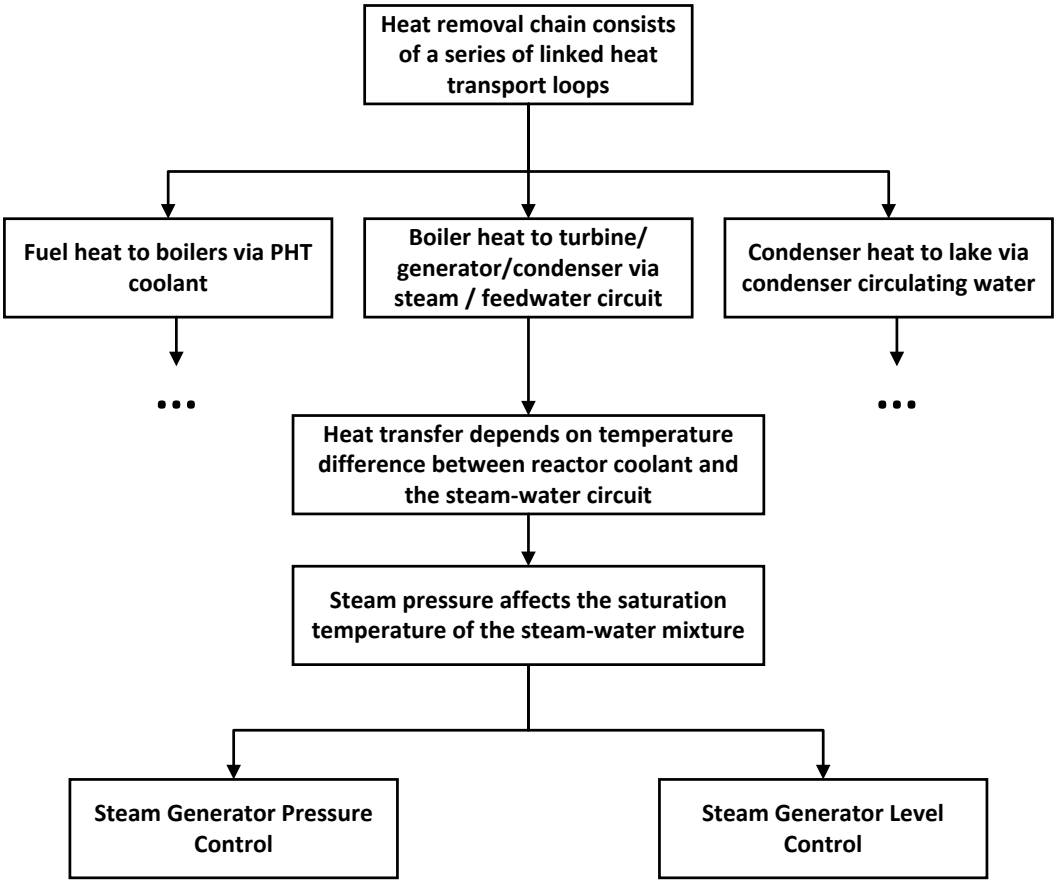


Figure 56 - Steam Generator Level Control Role Within Heat Removal Chain [39]

Figure 41 in section 7.4.4 shows a safety control structure for a typical nuclear power utility. For the purpose of engineering the technology at the utility level, a safety control structure that is focused on managing the technology to achieve one of the key safety goals, avoid overheating the fuel, is required. Figure 57 provides the required safety control structure diagram for the physical plant relative to the hazard of overheating the fuel. This is used as the basis for the hazard analysis in Section 11.2.2.2.3.

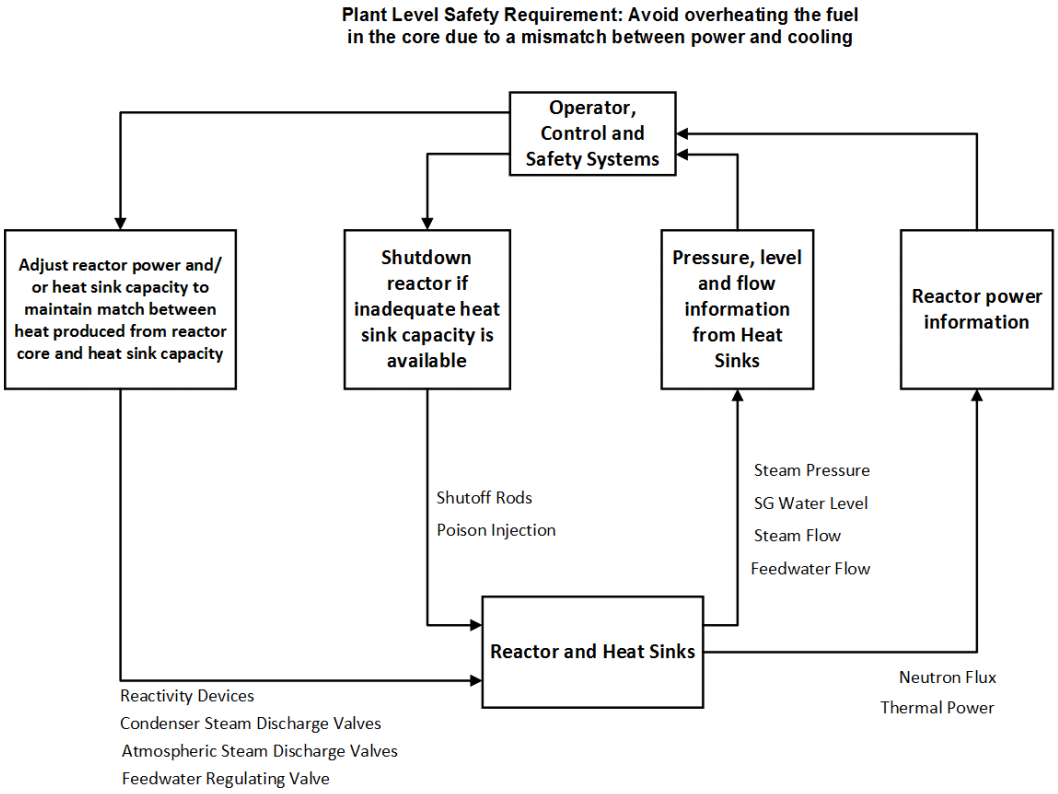


Figure 57 - Safety Control Structure of Plant Level Architecture Focused on Avoiding Overheating the Fuel

11.2.2.2.3 Technology Hazard analysis

The hazard analysis of the technology at the enterprise levels is done by following the hazard analysis steps defined in Section 6.2:

- Define the safety control structure
- Determine unsafe control actions
- Determine potential causes of unsafe control actions
- Identify design features to address causes of unsafe control actions

Safety Control Structure

Figure 57 shows a safety control structure diagram at the plant level focused on the key safety requirement of avoidance of overheating of the fuel.

Unsafe Control Actions

From Figure 57, it can be seen that the control actions that can be taken are:

- Raise/lower power
- Raise/lower flow
- Open/close ASDV, and
- Drop/remove rods

Each is these control actions are analyzed to determine under what conditions the control action is unsafe. The four scenarios by which a control action can be unsafe as described in Section 6.2 are used to identify the unsafe control actions. Table 7 through Table 14 identify the unsafe control actions for all the above control actions.

Control Action	Reactor Power vs Reactor Power Setpoint	Thermal Power vs Heat Sink Capacity	Reactor Power vs Trip Setpoint 1	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?
Raise Power	GT	GT	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
	EQ	GT	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
	LT	GT	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y

Table 7 - Unsafe Control Actions for Raise Power

Control Action	Reactor Power vs Reactor Power Setpoint	Thermal Power vs Heat Sink Capacity	Reactor Power vs Trip Setpoint 1	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?
Lower Power	GT	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
	EQ	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
	LT	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N

Table 8 - Unsafe Control Actions for Lower Power

Control Action	Reactor Power vs Reactor Power Setpoint	Thermal Power vs Heat Sink Capacity	Reactor Power vs Trip Setpoint 1	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?
Increase Flow	GT	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	N	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	N	N	N
	EQ	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	N	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	N	N	N
	LT	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	N	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	N	N	N

Table 9 - Unsafe Control Actions for Increase Flow

Control Action	Reactor Power vs Reactor Power Setpoint	Thermal Power vs Heat Sink Capacity	Reactor Power vs Trip Setpoint 1	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?
Lower Flow	GT	GT	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
	EQ	GT	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
	LT	GT	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	Y	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	P	N	Y
			GT	Y	N	Y	N	Y

Table 10 - Unsafe Control Actions for Lower Flow

Control Action	Reactor Power vs Reactor Power Setpoint	Thermal Power vs Heat Sink Capacity	Reactor Power vs Trip Setpoint 1	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?
Open ASDV	GT	GT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
	EQ	GT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
	LT	GT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
		EQ	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y
		LT	LTE	N	N	N	N	Y
			GT	Y	N	Y	N	Y

Table 11 - Unsafe Control Actions for Open ASDV

Control Action	Reactor Power vs Reactor Power Setpoint	Thermal Power vs Heat Sink Capacity	Reactor Power vs Trip Setpoint 1	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?
Close ASDV	GT	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	N	N	N
	EQ	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	N	N	N
	LT	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	N	N	N

Table 12 - Unsafe Control Actions for Close ASDV

Control Action	Reactor Power vs Reactor Power Setpoint	Thermal Power vs Heat Sink Capacity	Reactor Power vs Trip Setpoint 1	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?
Drop Rods	GT	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
	EQ	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
	LT	GT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	Y	N	N	N

Table 13 - Unsafe Control Actions for Drop Rods

Control Action	Reactor Power vs Reactor Power Setpoint	Thermal Power vs Heat Sink Capacity	Reactor Power vs Trip Setpoint 1	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?
Remove Rods	GT	GT	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N
	EQ	GT	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N
	LT	GT	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N
		EQ	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N
		LT	LTE	N	N	N	N	N
			GT	Y	N	Y	N	N

Table 14 - Unsafe Control Actions for Remove Rods

The collection of unsafe control actions can be simplified to:

- Not providing “Lower Power” or not providing “Drop Rods” OR not providing “Close ASDV” or providing “Remove Rods” when:
  - Reactor power > trip setpoint

- Providing “Raise Power” or “Lower Flow” or “Open ASDV” when:
  - Reactor power > trip setpoint or
  - Thermal power >= heat sink capacity or
  - Reactor power >= setpoint

Causes of Unsafe Control Actions

Table 15 shows the potential causes of the above unsafe control actions based on the generic causes of unsafe control actions given in Sections 6.2 and 6.3.

	Model Element	Generic Causes of Unsafe Control Actions	Not Providing "Lower Power" or "Drop Rods" when Reactor power > trip setpoint	Providing "Raise Power" or "Lower Flow" or "Open ASDV" when (reactor power > trip setpoint) or (thermal power >= heat sink capacity) or (reactor power >= setpoint)
1	Controller Related	Control input or external information wrong or missing	- incorrect trip setpoint provided to operator - operator did not correctly understand the required setpoint to be set - changes to the setpoint not communicated to operator in a timely manner	- incorrect setpoint provided to operator - operator did not correctly understand the required setpoint to be set - changes to the setpoint not communicated to operator in a timely manner
2		Inadequate control algorithm (flaws in creation, process changes, incorrect modification or adaption)	- error in specifying trip algorithm - error in implementation of trip logic - inadequate V&V to detect error in trip logic - changes to control logic not implemented in a timely manner	- error in specifying control algorithm - error in implementation of control algorithm - inadequate V&V to detect error in control algorithm - changes to control alogorithm not implemented in a timely manner
3		Process model inconsistent, incomplete or incorrect	- error in specification of process model - error in implementation of process model logic - changes to process model logic not implemented in a timely manner - time lags and inaccuracies not accounted for in the specification of the process model	- error in specification of process model - error in implementation of process model logic - changes to process model logic not implemented in a timely manner - time lags and inaccuracies not accounted for in the specification of the process model
4		Inappropriate, ineffective or missing control action	- communication of setpoint or setpoint changes to operator not done - communication of setpoint was unclear - delays in setting new setpoint	- communication of setpoint or setpoint changes to operator not done - communication of setpoint was unclear - delays in setting new setpoint
5		Feedback delays		
6		Inadequate or missing feedback		
7	Actuator Factors	Inadequate operation of actuator	- communication of setpoint or setpoint changes to operator not done - communication of setpoint was unclear - delays in setting new setpoint	- communication of setpoint or setpoint changes to operator not done - communication of setpoint was unclear - delays in setting new setpoint
8		Delayed operation of actuator	- delayed transmission of control action by HMI	- delayed transmission of control action by HMI
9	Controlled Process Factors	Controlled process input missing or wrong		
10		Component failures	- component failures	- component failures
11		Changes to controlled process over time		
12		Unidentified or out-of-range distrubance to controlled process		
13		Controlled process output contributes to system hazard		
14		Conflicting control action from other controller		
15	Sensor Factors	Feedback delays		
16		Measurement inaccuracies	- incorrect gain - incorrect compensation of flux detector signal	- incorrect gain - incorrect compensation of flux detector signal
17		Incorrect or no information provided		
18		Inadequate operation of sensor	- failures in sensors, communication lines or power	- failures in sensors, communication lines or power

Table 15 - Causes of Unsafe Control Actions

Design Features to Deal with Causes of Unsafe Control Actions

From Table 15, the set of potential causes of an unsafe control action are as follows:

1 incorrect setpoint provided to operator
2 operator did not correctly understand the required setpoint to be set
3 changes to the setpoint not communicated to operator in a timely manner
4 error in specifying trip algorithm
5 error in implementation of trip logic
6 inadequate V&V to detect error in trip logic
7 changes to control logic not implemented in a timely manner
8 error in specification of process model
9 error in implementation of process model logic
10 changes to process model logic not implemented in a timely manner
11 time lags and inaccuracies not accounted for in the specification of the process model
12 communication of setpoint or setpoint changes to operator not done
13 communication of setpoint was unclear

14 delays in setting new setpoint
15 loss of power in automated controller HMI
16 error in automated controller HMI
17 delayed transmission of control action by HMI
18 component failures
19 incorrect gain
20 incorrect compensation of flux detector signal
21 failures in sensors, communication lines or power

Appendix 6 lists the above causes and then identifies design features to deal with each cause. The design features are based on the IAEA principles in Appendix 3, and also other typical design features used to deal with each cause.

The summary of the resulting design features is as follows:

Minimize Human Error

- All activities important to safety shall be carried out in accordance with written procedures to ensure that the plant is operated within the established operational limits and conditions.
- Aspects of the working environment that influence human performance factors (such as workload or fatigue) and the effectiveness and fitness of personnel for duty shall be identified and controlled.
- Assumptions on operations and maintenance performance necessary to achieve safety are clearly documented
- Automatic systems are provided that would safely shut down the reactor, maintain it in a shut down and cooled state, and limit any release of fission products that might possibly ensue, if operating conditions were to exceed predetermined set points.
- Normal plant operations are controlled by detailed, validated and formally approved procedures
- Establish a program to ensure personnel assigned to safety related activities have the necessary competencies to perform the activities assigned to them
- Establish a staff health policy that ensures staff are fit for duty
- Establish a staffing plan that ensures that sufficient competent staff are available to perform safety related activities

- Establish policies for scheduling of personnel for safety related activities to ensure that sufficient time is allocated to adequately perform the activities
- Written communication shall be preferred and spoken communication shall be minimized. If spoken communication is used, attention shall be given to ensuring that spoken instructions are clearly understood.

High Quality, Safe Design

- Compliance with appropriate codes and standards
- Conservative design, construction and testing practices commensurate with safety objectives
- Design margins established to account for unanticipated failures.
- Hazards shall be eliminated if possible
- Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.
- Technical specifications for items important to safety shall be developed using appropriate methods that result in complete and correct specifications of safety requirements.
- The design of items important to safety shall take into account the attributes of manufacturability, constructability and install-ability to ensure that the probability of introduction of undetected errors is commensurate with the level of risk of errors.
- Operating experience from the design, construction and operation of similar plants shall be taken into account.
- Operations and maintenance personnel are involved in effective design reviews to ensure that assumptions on operations and maintenance performance are achievable
- Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents
- Procured items important to safety shall be qualified as being compliant with safety requirements
- Proven methods of manufacturing and construction
- Quality assurance applied to ensure with high level of confidence that safety requirements and objectives are met

- Reliability targets are assigned to safety systems or functions. The targets are established on the basis of the safety objectives and are consistent with the roles of the systems or functions in different accident sequences. Provision is made for testing and inspection of components and systems for which reliability targets have been set.
- Remaining hazards shall be controlled to make their probability of occurrence as low as reasonably achievable
- Robust technical justification for the inspection and maintenance program.
- Safety components and systems are chosen that are qualified for the environmental conditions that would prevail if they were required to function. The effects of ageing on normal and abnormal functioning are considered in design and qualification.
- Safety related structures, system and components are subject to regular maintenance, inspection and testing as necessary to ensure that they perform consistent with safety requirements over the life of the plant
- The qualification of procured items shall include a hazard analysis to determine if there are any new hazards introduced by the use of the item
- Designate an individual to be responsible for the safety of the plant design

Reliable Ongoing Safety Performance

- Establish and implement a commissioning program that demonstrates that the plant as built is compliant with all design assumptions and licensing conditions
- Establish operating and maintenance procedures necessary to keep the plant operating within its safe operating envelope and validate the procedures as part of the commissioning program
- Establish a maintenance program for all equipment that is related to performing safety functions in the plant
- Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner.
- Establish a program to investigate events with significant implications for safety and take effective actions to avoid reoccurrence of the events.
- Establish a safety management system that ensuring the continuing safety of the plant design.
- Establish an ageing management program to maintain the performance of structures, systems and components that have an impact on safety

- Establish and implement a program for the planning and execution of online and offline maintenance and design modification activities
- Establishment of a program for identification and effective communication with parties interested in the safety of the plant
- Establishment of a risk management program that ensures that risks are identified, analyzed and reduced to levels as low as reasonably achievable.
- Establishment of a safety management system that takes into account the safety significance of changes
- Establishment of a set of programs necessary to achieve and maintain safety along with the establishment of an effective management system for the programs
- Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements
- Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements
- The operating organization shall encourage plant personnel to have a questioning attitude and to make appropriate and conservative decisions, so as to minimize risk and to maintain the plant in a safe condition.

11.2.2.3 Utility Level - Business Process View

This Section applies the SEE approach to the business process view of the enterprise. For the business process view of the enterprise the following steps are done (as represented in Figure 54):

- The safety requirements for the business processes are established
- The architecture of the business processes is defined
- A hazard analysis of the business processes is performed

Note that all three of these outcomes are limited in scope, as they focus on establishing the context for the engineering of the Periodic Safety Review process in Section 11.2.4.

11.2.2.3.1 Business Process Safety Requirements

Figure 32 and Figure 38 show two representations of the overall business process architecture of a typical nuclear utility based on the Nuclear Energy Institute document "The Standard Nuclear Performance Model - A Process Management Approach" [41]. Figure 32 shows a hierarchical decomposition of the major processes. Figure 38 shows a high level view of the processes with some of the major dependencies between processes shown. The processes are grouped into core processes, enabling processes and management processes.

Process LP002, "Provide Performance Monitoring and Improvement Services", in Figure 38 is defined as "All actions taken to verify effectiveness and compliance with regulations and codes, including those in support of internal decisions which assist in assuring compliance. This activity would include self-assessment, any actions taken to identify, make root cause determinations and implement the corrective action program as well as associated trending activities. It also includes human performance/human factors/error prevention and reduction and knowledge management activities. It also includes required audits and inspections that verify regulatory compliance/conformance excluding nuclear vendor qualification (Cost of audits needed for selection and ongoing management of vendors should be reflected in MS process costs). Otherwise nuclear quality assurance program implementation and maintenance activities are to be included." [22]

As per the IAEA document "Safety of nuclear power plants: commissioning and operation"[32] one of the requirements for managing operational safety is to perform periodic safety reviews (PSRs) which is an element of the LP002 process. The requirements on periodic safety reviews include:

- Systematic safety assessments of the plant, in accordance with the regulatory requirements, shall be performed by the operating organization throughout the plant's operational lifetime, with due account taken of operating experience and significant new safety related information from all relevant sources.
- PSR provides an effective way to obtain an overall view of actual plant safety and the quality of the safety documentation, and to determine reasonable and practical modifications to ensure safety or improve safety to an appropriate high level. To do this, the PSR needs to identify any lifetime limiting features at the plant in order to plan future modifications and to determine the timing of future reviews.

- On the basis of international experience, it is reasonable to perform a PSR about ten years after the start of plant operation, and then to undertake subsequent PSRs at ten year intervals until the end of operation.

Within the Canadian regulatory framework, as per Table 6, the requirements for periodic safety reviews are documented in REGDOC 2.3.3 Periodic Safety Review [57]. REGDOC 2.3.3 is based on the IAEA specific safety guide "Periodic Safety Review for Nuclear Power Plants"[60] which requires that the review be based on 14 different safety factors as follows:

Safety factors relating to the plant

(1) Plant design;

(2) Actual condition of structures, systems and components (SSCs) important to safety;

(3) Equipment qualification;

(4) Ageing.

Safety factors relating to safety analysis

(5) Deterministic safety analysis;

(6) Probabilistic safety assessment;

(7) Hazard analysis.

Safety factors relating to performance and feedback of experience

(8) Safety performance;

(9) Use of experience from other plants and research findings.

Safety factors relating to management

(10) Organization, the management system and safety culture;

(11) Procedures;

(12) Human factors;

(13) Emergency planning.

Safety factors relating to the environment

(14) Radiological impact on the environment.

11.2.2.3.2 Business Process Architecture

As described in the previous Section, Figure 32 and Figure 38 show the overall business process architecture of a typical nuclear utility.

11.2.2.3.3 Business Process Hazard analysis

Safety Control Structure

Figure 41 in section 7.4.4 shows a safety control structure for a typical nuclear power utility. For the purpose of this example, a safety control structure that is focused on managing the performance monitoring and continuous improvement function is required since the Periodic Safety Review process is part of this function. Figure 58 provides the required safety control structure diagram for this function. The "process being controlled" is the combination of all functions[9] to design, construct, operate, maintain and modify the nuclear power plant and its control systems. Also included is the function to monitor all the aforementioned functions and technologies. The "controller" in the diagram is the governance processes that makes decisions on necessary changes in order to address findings from the performance monitoring function.

For the performance monitoring and continuous improvement function, the hazardous state of the utility is being in a state where there is a non-compliance

[9] Note that each function is implemented with a set of business processes executed by defined organizations supported by technologies and overseen in accordance with defined governance.

with regulatory requirements or non-compliance with the assumptions upon which the safety report for the plant was based.

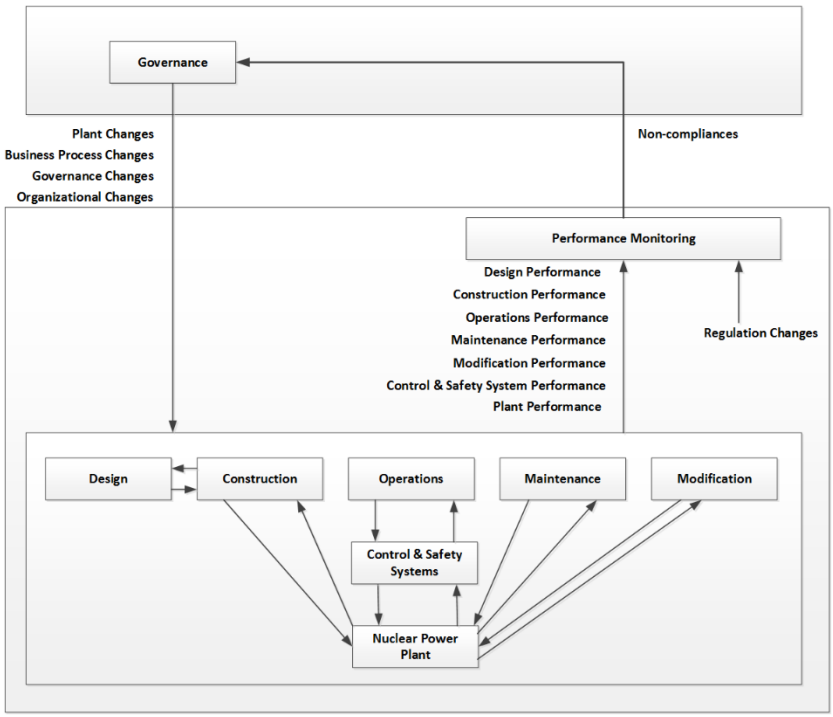


Figure 58 - Safety Control Structure for Performance Monitoring & Continuous Improvement

Unsafe Control Actions

From Figure 58 it can be seen that the control actions are to request changes to either the plant, the business processes, the organization or the governance associated with one or more function. Table 16 documents the results of the analysis of these control actions. It analyzes the control actions separately for different states. The relevant states are whether the utility is fully compliant with all regulatory and safety requirements, and whether any non-compliances were found by the periodic safety review process.

Control Action	State of Compliance of Plant / Business Process / Organization / Governance	Non-Compliances Found?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?	Comments
Change Plant / Business Process / Organization / Governance	Non-Compliant	Y	Y	N	Y	Y	Unsafe if the state of the utility is non-compliant and changes are not made in a timely manner to bring the utility back into a compliant state
		N	Y	N	Y	Y	
	Compliant	NA	N	Y, if changes result in non-compliance	N	N	Not unsafe if utility is already in a compliant state, unless changes are made that make the utility non-compliant
		N	N	Y, if changes result in non-compliance	N	N	

Table 16 - Unsafe Control Actions for Change Plant / Business Process / Organization / Governance

The two unsafe control actions identified are:

1) Changes are not made in a timely manner to bring the utility into a compliant state, and
2) Changes are made that result in the utility being non-compliant

Causes of Unsafe Control Actions

The above two unsafe control actions were then assessed against the generic causes of unsafe control actions given in Sections 6.2 and 6.3. Table 17 documents the results of this assessment.

	Model Element	Generic Causes of Unsafe Control Actions	Unsafe if the state of the utlity is non-compliant and changes are not made in a timely manner to bring the utility back into a compliant state	Not unsafe if utility is already in a compliant state, unless changes are made that make the utility non-compliant
1	Controller Related	Control input or external information wrong or missing	- regulatory requirements are not clearly specified - regulatory requirements are not commonly understood - changes to regulatory requirements are not communicated in a timely manner	- regulatory requirements are not clearly specified - regulatory requirements are not commonly understood - changes to regulatory requirements are not communicated in a timely manner
2		Inadequate control algorithm (flaws in creation, process changes, incorrect modification or adaption)	- changes to regulatory requirements are not assessed and acted upon in a timely manner - scope of change identified inadequate to achieve compliance	- changes to regulatory requirements are not assessed and acted upon in a timely manner - scope of change identified inadequate to achieve compliance
3		Process model inconsistent, incomplete or incorrect	- incorrect understanding of current processes	- incorrect understanding of current processes
4		Inappropriate, ineffective or missing control action	- inadequate resources allocated to implement changes - inadequate priority given to making changes	- inadequate resources allocated to implement changes - inadequate priority given to making changes
5		Feedback delays	- incorrect information about current state of utlity is provided	- incorrect information about current state of utlity is provided
6		Inadequate or missing feedback	- assessments not performed to detect non-compliances	
7	Actuator Factors	Inadequate operation of actuator	- unclear communications about nature of changes required - request for changes not supported by adequate resources	
8		Delayed operation of actuator		
9	Controlled Process Factors	Controlled process input missing or wrong	- request for change ignored - request for change not given adequate priority - scope of change required not understood adequately	
10		Component failures	- change implemented poorly	- change implemented poorly
11		Changes to controlled process over time	- scope of change inconsistent with current state of utility	- scope of change inconsistent with current state of utility
12		Unidentified or out-of-range distrubance to controlled process		
13		Controlled process output contributes to system hazard	- implementation of change results in hazard not previously present	
14		Conflicting control action from other controller		
15	Sensor Factors	Feedback delays	- assessment reports not produced in a timely manner	
16		Measurement inaccuracies	- assessors not qualified - assessment based on inaccurate information	
17		Incorrect or no information provided	- documentation of current state not up-to-date	- documentation of current state not up-to-date
18		Inadequate operation of sensor		

Table 17 - Causes of Unsafe Control Actions

Design Features to Deal with Causes of Unsafe Control Actions

From Table 17, the set of potential causes of an unsafe control action are as follows:

1 regulatory requirements are not clearly specified
2 regulatory requirements are not commonly understood
3 changes to regulatory requirements are not communicated in a timely manner
4 changes to regulatory requirements are not assessed and acted upon in a timely manner
5 scope of change identified inadequate to achieve compliance"
6 incorrect understanding of current processes
7 inadequate resources allocated to implement changes
8 inadequate priority given to making changes
9 incorrect information about current state of utility is provided
10 assessments not performed to detect non-compliances
11 unclear communications about nature of changes required
12 request for change ignored
13 change implemented poorly
14 scope of change inconsistent with current state of utility

15 implementation of change results in hazard not previously present
16 assessment reports not produced in a timely manner
17 assessors not qualified
18 assessment based on inaccurate information
19 documentation of current state not up-to-date

Appendix 6 lists the above causes and then identifies design features to deal with each cause. The design features are based on the IAEA principles in Appendix 3, and also other typical design features used to deal with each cause.

The summary of the resulting design features is as follows:

Effective Regulation

- The government shall promulgate laws and statutes to make provision for an effective governmental, legal and regulatory framework for safety
- complete and clear set of regulatory documents

Safety Management

- Establish accountabilities for senior management to establish a safety management program
- Establish accountabilities for senior management to effectively implement the safety management program
- Expectations that the safety management system be developed, applied and continuously improved shall be established.
- The safety management system shall be integrated into the overall management system
- Documented safety management plan
- Establishment of a safety management system that is clearly documented
- Compliance of safety management plan with industry standards
- Clear documentation of the engineering process
- Effective management oversight of the engineering process
- Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety
- Establishment of a document and records management system so that all safety related documents are controlled, and the correct version of documents and records are available to personnel requiring them

- Establish a safety management system that ensuring the continuing safety of the plant design.
- Establishing processes, organizations and governance in compliance with standards for safety, quality and management.
- Establishment of an adequate emergency preparedness program.
- Adequate configuration management

Leadership

- Establish accountabilities for managers to support and advocate a strong safety culture
- Clear definition of accountabilities for managers responsible for the safety of the plant during siting, design, construction, commissioning, operation and decommissioning.
- Clearly established expectations on the leadership to communicate, demonstrate and reinforce the expected safety behaviour
- Designate an individual to be responsible for the safety of the plant design
- Adequate management oversight of assessments
- Management oversight to ensure that personnel have required qualifications

Competencies

- Understanding of all personnel on their role in the safety management plan
- Competencies required for each design activity are clearly defined
- The management system shall ensure that personnel assigned to design activities have the pre-requisite competencies to perform those activities
- Establish a program to ensure personnel assigned to safety related activities have the necessary competencies to perform the activities assigned to them
- Establish a staffing plan that ensures that sufficient competent staff are available to perform safety related activities
- Establish a staff health policy that ensures staff are fit for duty
- Understanding of all personnel on their role in the safety management plan
- Comprehensive training of personnel in the expectations of the engineering process
- Programs to communicate and train personnel in the safety policies
- Personnel involved with safety related activities have the competencies necessary to perform their duties

- specific training on regulatory requirements for relevant personnel

Assessments and Audits

- Assessments and audits of compliance with safety management plan
- Periodic safety review program including review of operational experience inside and outside the organization
- Establish periodic safety reviews of the plant, processes, organizations and governance
- Establish continuous improvement process taking input from periodic safety review and operational experience both internal and external to the organization
- Safety assessment done before construction and operation begins
- Safety assessment is performed independently and documented in a third party reviewable manner
- Continuous improvement program focused on operational safety
- regular review of changes to regulatory requirements
- clear documentation of actions required to respond to any non-compliances
- sufficient assessments of compliance of processes with documented expectations
- Adequate verification and validation of implementations to provide confidence that change has been implemented consistent with safety and quality requirements

Priorities

- Establishing governance that ensures adequate resources and funding are available to achieve and maintain safety including during decommissioning and for radioactive waste disposal
- Establish policies for scheduling of personnel for safety related activities to ensure that sufficient time is allocated to adequately perform the activities
- Clearly established policy and governance with respect to the expectations for taking safety into account in all decisions
- Safety policies establishing the priority for safety and the standards to be met for all safety related activities
- Possibility of human error is taken into account

- priority given to identify and implement changes necessary to respond to regulatory changes
- adequate priority is assigned to changes necessary to implement changes required to achieve compliance with regulatory and safety requirements

Operational Excellence

- Operational excellence is achieved by:
    - augmenting safety culture and defence in depth;
    - improving human performance;
    - maintaining excellent material condition and equipment performance;
    - using self-assessments and peer reviews; exchanging operating experience and other information around the world;
    - increasing application of PSAs; and extending the implementation of severe accident management.

11.2.3 Steam Generator Level Control Engineering

Control of the steam generator is done by two control functions:

- Steam Generator Level Control
- Steam Generator Pressure Control

The steam generator level control system measures water level, and manipulates feedwater flow to maintain the water level in the steam generator within defined limits.

In this example, a simplified version of steam generator level control will be analyzed. A simple control system that measures water level and manipulates feedwater flow to achieve a defined water level setpoint will be assumed. An actual steam generator level control system would vary the setpoint based on reactor power or turbine power levels and would also take feedwater flow and steam flow into account in manipulating the feedwater flow.

Figure 59 provides a graphical representation of the steps taken in the engineering of the Steam Generator Level Controls. The figure shows the main outcomes of each step in the SEE process.

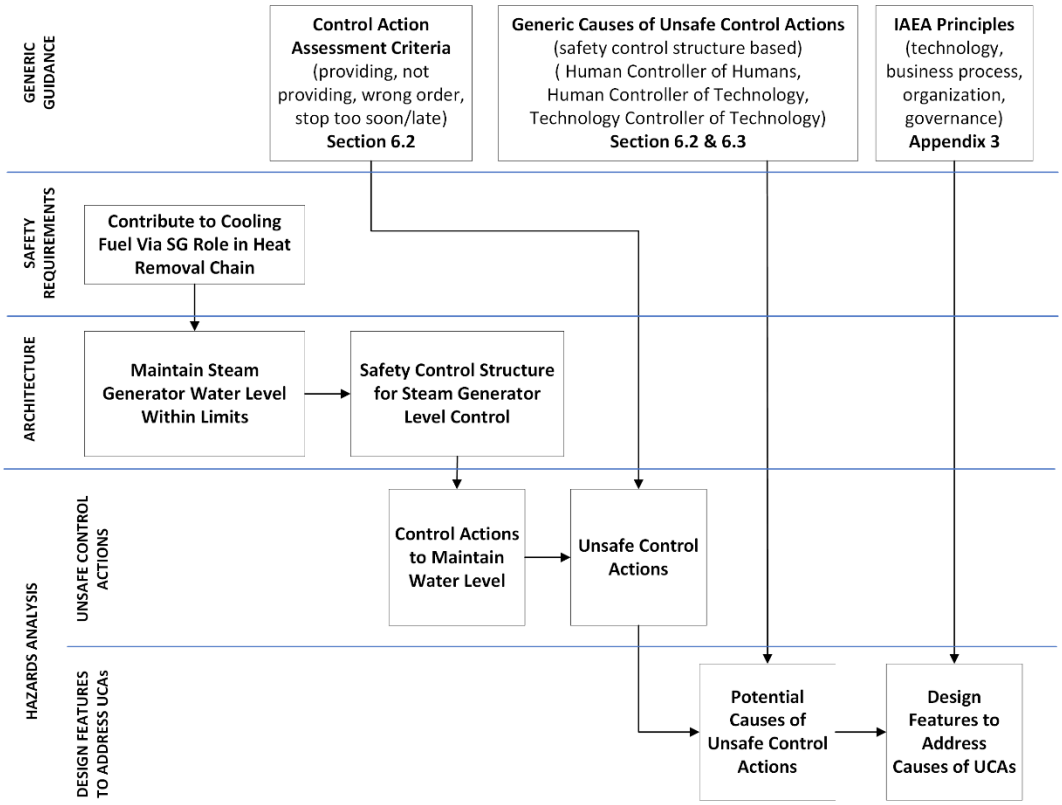


Figure 59 - Engineering of Steam Generator Level Controls

11.2.3.1 Steam Generator Level Control Safety Requirements

As described in Section 11.2.2.2.2 , the steam generator plays a key role in maintaining heat sinks to prevent the fuel from overheating and melting. Maintaining the water level within defined limits is one of the functions required to achieve this overall safety function.

Figure 60 illustrates the overall requirement for controlling the water level in the steam generator.

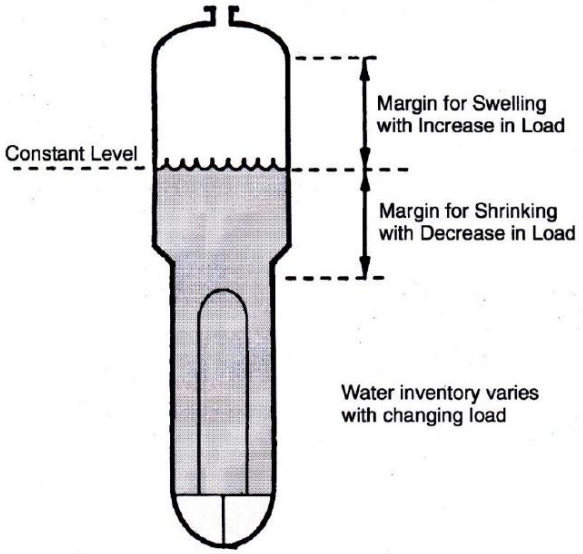


Figure 60 Steam Generator Level Control – Constant Level [39]

11.2.3.2 Steam Generator Level Control Architecture

Figure 37 shows the architecture of the major control systems. Historically the steam generator was called a boiler, and hence the steam generator level control system is called boiler level control in the figure. As mentioned, this example is based on a simplified steam generator control system that controls the feedwater flow based on water level only. Figure 37 shows that an actual system would also take feedwater flow and steam pressure into account.

11.2.3.3 Steam Generator Level Control Hazard analysis

Safety Control Structure

Figure 61 provides a safety control structure for the simplified steam generator control system. The controller issues control actions to either raise or lower the flow of feedwater to the steam generator based on sensor input of the water level in the steam generator.

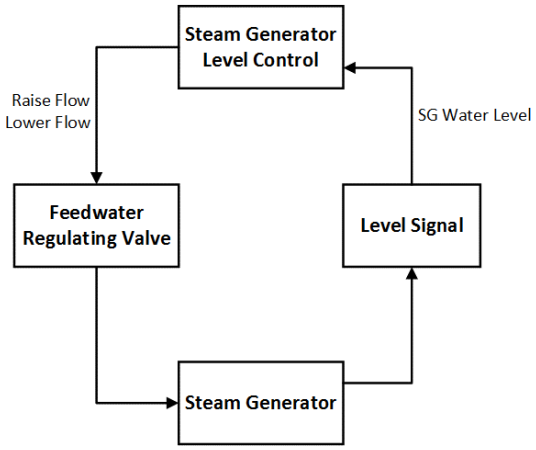


Figure 61 - Steam Generator Level Control Safety Control Structure

Unsafe Control Actions

From Figure 61, it can be seen that the control actions that can be taken are raise flow or lower flow.

Each is these control actions is analyzed to determine under what conditions the control action is unsafe. The four scenarios by which a control action can be unsafe as described in Section 6.2 are used to identify the unsafe control actions. Table 18 identifies the unsafe control actions for the above control actions.

Control Action	Water Level vs Setpoint +/- Margin	Is Starting State Hazardous?	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?	Comments
Increase Flow	GT	N	N	N	N	N	Unsafe if Increase Flow CA not effectively provided when level is below sepoint - margin
	EQ	N	N	N	N	N	
	LT	Y	Y	N	Y	Y	
Lower Flow	GT	N	N	N	N	N	Unsafe if Lower Flow CA is taken when level is below setpoint - margin
	EQ	N	N	N	N	N	
	LT	Y	N	Y	Y	Y	

Table 18 - Unsafe Control Actions for SG Level Control

Causes of Unsafe Control Actions

Table 19 shows the potential causes of the above unsafe control actions based on the generic causes of unsafe control actions given in Sections 6.2 and 6.3.

Model Element	Generic Causes of Unsafe Control Actions	Not Providing Increase Flow when level is below sepoint - margin	Providing Decrease Flow when level is below setpoint - margin
Controller Related	Control input or external information wrong or missing	- incorrect setpoint set - incorrect margin set - required changes to setpoint or margin not made in a timely manner - control algorithm not specified correctly - control algorithm not implemented correctly - automated controller not able to meet performance requirements - required changes to control algorithm not implemented in a timely manner - failure of autmated controller	- incorrect setpoint set - incorrect margin set - required changes to setpoint or margin not made in a timely manner - control algorithm not specified correctly - control algorithm not implemented correctly - automated controller not able to meet performance requirements - required changes to control algorithm not implemented in a timely manner - failure of autmated controller - loss of power to automated controller - mismatch between state of model and actual level in steam generator
	Inadequate control algorithm (flaws in creation, process changes, incorrect modification or adaption)		
	Process model inconsistent, incomplete or incorrect		
	Inappropriate, ineffective or missing control action		
	Feedback delays		
	Inadequate or missing feedback		
Actuator Factors	Inadequate operation of actuator	- error in implementation of feedwater control valve - failure of feedwater control valve - loss of power to feedwater control valve	- error in implementation of feedwater control valve - failure of feedwater control valve - loss of power to feedwater control valve
	Delayed operation of actuator		
Controlled Process Factors	Controlled process input missing or wrong		
	Component failures		
	Changes to controlled process over time		
	Unidentified or out-of-range distrubance to controlled process		
	Controlled process output contributes to system hazard		
	Conflicting control action from other controller		
Sensor Factors	Feedback delays	- error in implementation of level sensor - failure of level sensor - loss of power to level sensor - level sensor is inaccurate	- error in implementation of level sensor - failure of level sensor - loss of power to level sensor - level sensor is inaccurate
	Measurement inaccuracies		
	Incorrect or no information provided		
	Inadequate operation of sensor		

Table 19 - Causes of Unsafe Control Actions

Design Features to Deal with Causes of Unsafe Control Actions

Table 19, the set of potential causes of an unsafe control action are as follows:

1. incorrect setpoint set
2. incorrect margin set
3. required changes to setpoint or margin not made in a timely manner
4. control algorithm not specified correctly
5. control algorithm not implemented correctly

6. automated controller not able to meet performance requirements
7. required changes to control algorithm not implemented in a timely manner
8. failure of automated controller
9. loss of power to automated controller
10. mismatch between state of model and actual level in steam generator
11. error in implementation of feedwater control valve
12. failure of feedwater control valve
13. loss of power to feedwater control valve
14. error in implementation of level sensor
15. failure of level sensor
16. loss of power to level sensor
17. level sensor is inaccurate

Appendix 6 lists the above causes and then identifies design features to deal with each cause. The design features are based on the IAEA principles and also other typical design features used to deal with each cause.

The summary of the resulting design features is as follows:

High Quality Design

- Components, structures, and systems used during startup, low power and shutdown operations are designed to maintain or restore the reactivity control, decay heat removal, and the integrity of the fission product barriers, so as to prevent the release of radioactive material resulting from accidents initiated during those operations.
- Conservative design, construction and testing practices commensurate with safety objectives
- Compliance with appropriate codes and standards
- Proven methods of manufacturing and construction
- Quality assurance applied to ensure with high level of confidence that safety requirements and objectives are met
- Clear, complete and correct specifications for safety related equipment
- Technical specifications for items important to safety shall be developed using appropriate methods that result in complete and correct specifications of safety requirements.
- Procured items important to safety shall be qualified as being compliant with safety requirements
- The qualification of procured items shall include a hazard analysis to determine if there are any new hazards introduced by the use of the item

- Design margins established to account for unanticipated failures.
- robust design process
- robust V&V
- Design margins established to account for unanticipated failures.
- Clear interface between process designer and I&C designer
- effective V&V
- Effective design process
- Reliable sources of power
- Redundant sources of power
- diverse sources of power
- qualified components
- graded QA requirements commensurate with safety significance

Competencies

- Operation and maintenance staff are trained and qualified to perform their duties in accordance with approved procedures
- Training programs in place to ensure that personnel responsible for safety related tasks have the necessary competencies
- Equipment, instrumentation and diagnostic aids are available to operators, who may at some time be faced with the need to control the course and consequences of an accident beyond the design basis.
- Effective equipment qualification programs to provide confidence that equipment will satisfy its safety requirements
- Design utilizes defense-in-depth principle to achieve control, cool and contain with a high degree of confidence.
- The design takes into account interactions between systems to ensure that failures of systems providing redundant or diverse safety functionality do not have common cause failures.

Change Control

- Controlling changes to the design to ensure assurance that safety requirements are satisfied is maintained at the same level or better when changes are made to the design
- Establishment of controls on plant configuration that ensures changes to plant configuration are consistent with the established safe operating envelope

- Establishment of a design modification process that is compliant with relevant national and international standards, and is based on proven engineering practices
- Design modification process includes proper design and safety reviews, implementation and testing
- Effective OPEX and Timely Change Control
- Effective change control process
- prioritization of work based on safety impacts
- Impact assessment of all proposed changes from a safety perspective to identify the need for a change to the setpoint
- Effective use of OPEX to identify needed changes
- Effective change control process to implement changes in a timely manner

Maintenance

- Robust technical justification for the inspection and maintenance program.
- Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements
- Establish a maintenance program for all equipment that is related to performing safety functions in the plant
- Robust technical justification for the inspection and maintenance program.
- Establishment of controls over the configuration of the physical plant and its design including a limit on the number of temporary modifications and limits on the time they may be in effect
- Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements
- Effective preventive maintenance program
- Effective ageing management program

11.2.4 Periodic Safety Review (PSR) Process Engineering

Figure 62 provides graphical representations of the steps taken in the engineering of the Periodic Safety Review Process. The figure shows the main outcomes of each step in the SEE process.

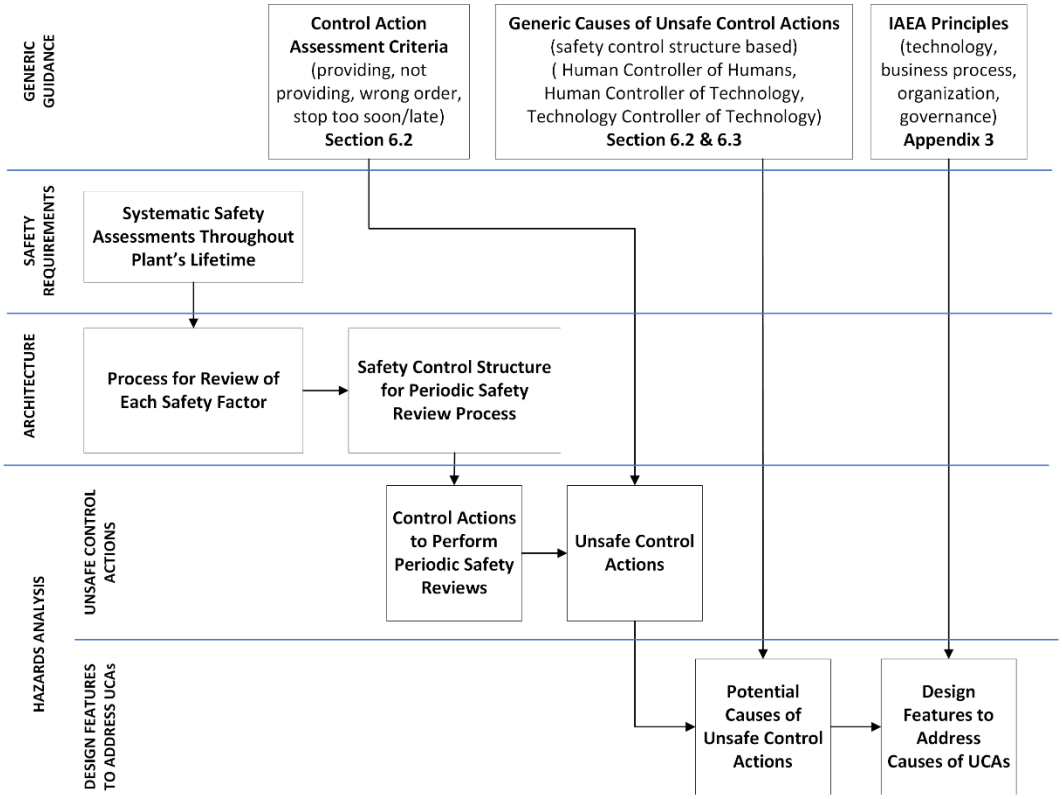


Figure 62 - Engineering of Periodic Safety Review Process

11.2.4.1 PSR Process Safety Requirements

As described in Section 11.2.2.3.3, the two unsafe control actions for the performance monitoring and continuous improvement function are:

1) Changes are not made in a timely manner to bring the utility into a compliant state, and
2) Changes are made that result in the utility being non-compliant

Since the periodic safety review process is a part of the overall function, the same unsafe control actions apply to the PSR process.

Specific requirements for the PSR process are in the IAEA document, Safety of nuclear power plants: commissioning and operation [32] where it states:

- "Systematic safety assessments of the plant, in accordance with the regulatory requirements, shall be performed by the operating organization

throughout the plant's operational lifetime, with due account taken of operating experience and significant new safety related information from all relevant sources".

- PSR provides an effective way to obtain an overall view of actual plant safety and the quality of the safety documentation, and to determine reasonable and practical modifications to ensure safety or improve safety to an appropriate high level. To do this, the PSR needs to identify any lifetime limiting features at the plant in order to plan future modifications and to determine the timing of future reviews.

- On the basis of international experience, it is reasonable to perform a PSR about ten years after the start of plant operation, and then to undertake subsequent PSRs at ten year intervals until the end of operation.

Within the Canadian regulatory framework, as per Table 6, the requirements for periodic safety reviews are documented in REGDOC 2.3.3 Periodic Safety Review [57]. REGDOC 2.3.3 is based on the IAEA specific safety guide "Periodic Safety Review for Nuclear Power Plants"[60] which requires that the review be based on 14 different safety factors as follows:

Safety factors relating to the plant

(1) Plant design;

(2) Actual condition of structures, systems and components (SSCs) important to safety;

(3) Equipment qualification;

(4) Ageing.

Safety factors relating to safety analysis

(5) Deterministic safety analysis;

(6) Probabilistic safety assessment;

(7) Hazard analysis.

Safety factors relating to performance and feedback of experience

(8) Safety performance;

(9) Use of experience from other plants and research findings.

Safety factors relating to management

(10) Organization, the management system and safety culture;

(11) Procedures;

(12) Human factors;

(13) Emergency planning.

Safety factors relating to the environment

(14) Radiological impact on the environment.

The inputs to be used for the assessment of each safety factor are also listed. For most factors, the inputs consist of a list of:

- Standards and requirements,
- Plant specific documents, and
- Operating experience information.

11.2.4.2 PSR Process Architecture

Figure 63 shows the steps involved in the review of each of the safety factors.

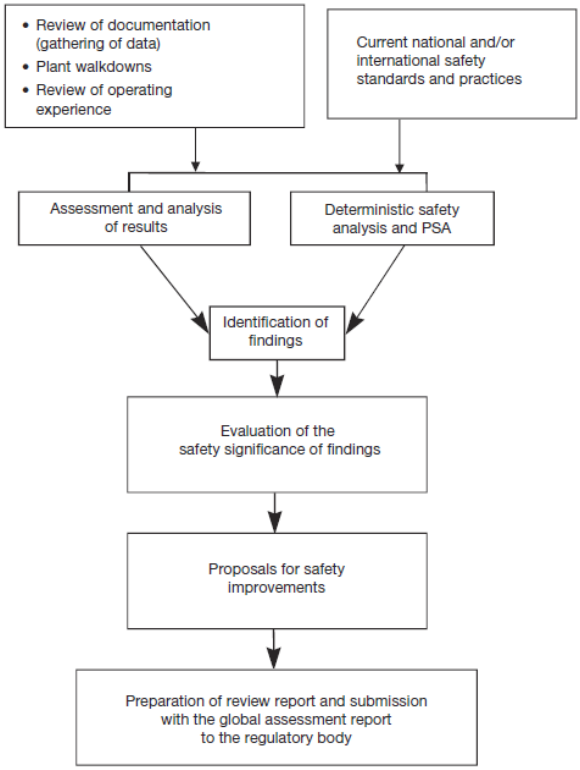


Figure 63 - Process for the Review of Each Safety Factor [60]

11.2.4.3 PSR Process Hazard analysis

Safety Control Structure

Figure 64 shows the safety control structure for the PSR process. Performance Monitoring and Continuous Improvement governance makes the decision to request the Periodic Safety review which provides feedback in the form of findings and recommendations. The PM & CI function would use this information to decide on required changes to the functions of the nuclear utility as per Figure 64.

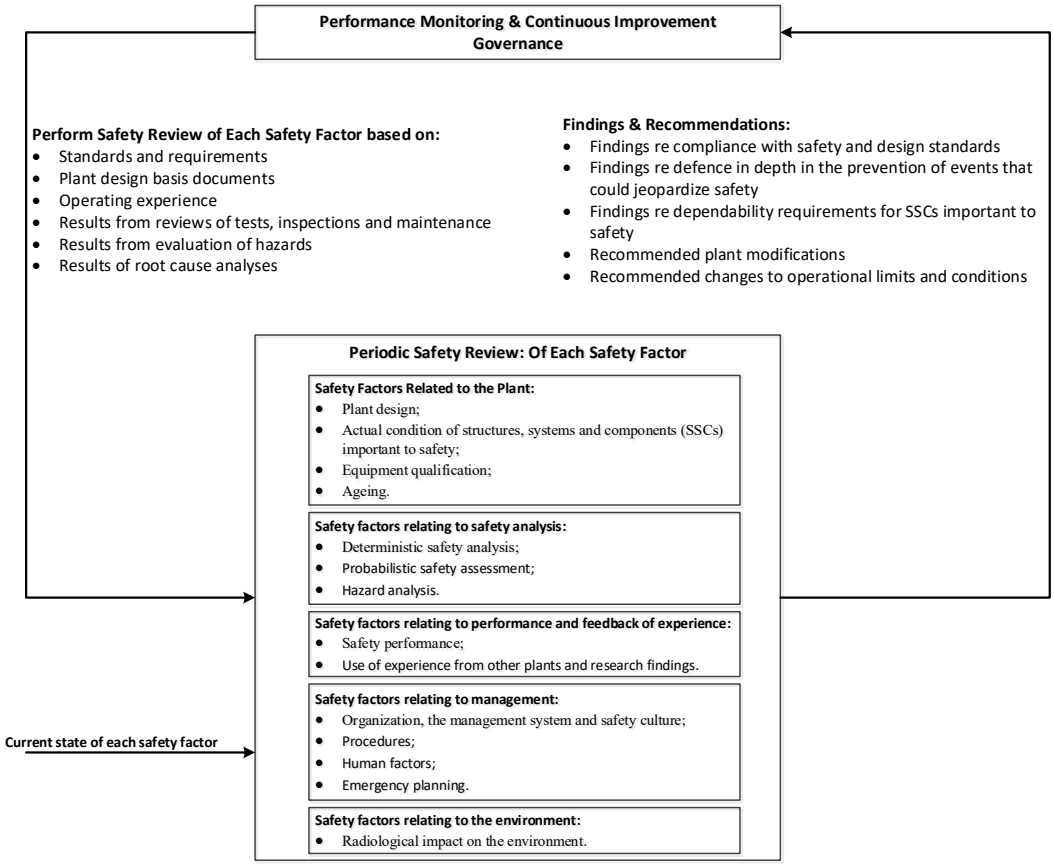


Figure 64 - Safety Control Structure for Periodic Safety Review Process

Unsafe Control Actions

From Figure 64, it can be seen that the control action that can be taken is Perform Periodic Safety Review. The control action was analyzed to determine under what conditions the control action is unsafe. The four scenarios by which a control action can be unsafe as described in Section 6.2 are used to identify the unsafe control actions. Table 20 identifies the unsafe control actions for the above control action.

Control Action	Availability of Opportunities	Findings	Does Not Providing the CA Cause a Hazard?	Does Providing the CA Cause a Hazard?	Does Wrong Timing/Order of CA Cause a Hazard?	Does Stopping the CA Too Soon or Applying it Too Long Cause a Hazard?	Comments
Perform Periodic Safety Review	Opportunities Available to be Found	Y	Y	N	Y	Y	Unsafe if Opportunities are Available to be Found and they are not found
		N	Y	Y	Y	Y	
	No Opportunities Available to be Found	Y	N	N	N	N	Not unsafe if there are no opportunities available to be found
		N	N	N	N	N	

Table 20 - Unsafe Control Actions for Periodic Safety Review Process

Causes of Unsafe Control Actions

Table 21 shows the potential causes of the above unsafe control actions based on the generic causes of unsafe control actions given in Sections 6.2 and 6.3.

			Perform Periodic Safety Review
			No findings when there are opportunities available
1	Controller Related	Control input or external information wrong or missing	- standards, requirements, plant design basis documents and/or any information required for review of a safety factor area either does not exist, is not current, is missing or is incorrect. - standards and/or requirements do not match the safety factor area as implemented
2		Inadequate control algorithm (flaws in creation, process changes, incorrect modification or adaption)	- no definition of the business process to conduct periodic safety reviews - decision makers not adequately trained in requirements for performing periodic safety reviews - inadequate budget allocated to support PSR - inadequate staffing of personel with the required skills for PSR - responsibility for initiating a PSR not defined - inadequate understanding by decision makers on the scope and personnel requirements necessary to conduct an effective PSR - inadequate priority given to conducting the PSR
3		Process model inconsistent, incomplete or incorrect	- perception that the current state of all safety factors is acceptable and hence scheduling a PSR is a low priority
4		Inappropriate, ineffective or missing control action	- lack of understanding on the frequency for conducting a PSR - priority and/or expectations for the performance of PSR not clearly communicated - responsibilities for performing PSR in each safety factor area is not clearly defined and/or communicated
5		Feedback delays	- lack of establishing effective performance measures that reflect the current state of each safety factor area
6		Inadequate or missing feedback	
7	Actuator Factors	Inadequate operation of actuator	- need to conduct PSR is not communicated in a timely manner to allow the needs to be incorporated into business plans
8		Delayed operation of actuator	- hiring of staff with the appropriate knowledge and skills results in delays to performance of the PSR
9	Controlled Process Factors	Controlled process input missing or wrong	- standards, requirements, plant design basis documents and/or any information required for review of a safety factor area either does not exist, is not current, is missing or is incorrect. - standards and/or requirements do not match the safety factor area as implemented
10		Component failures	- human error - organizations and personnel assigned to perform the pSR do not have the necessary skills and knowledge
11		Changes to controlled process over time	
12		Unidentified or out-of-range disturbance to controlled process	
13		Controlled process output contributes to system hazard	
14		Conflicting control action from other controller	
15	Sensor Factors	Feedback delays	
16		Measurement inaccuracies	
17		Incorrect or no information provided	- PSR findings and recommendations not communicated to requesters in a timely manner
18		Inadequate operation of sensor	

Table 21 - Causes of Unsafe Control Actions for Periodic Safety Review Process

Design Features to Deal with Causes of Unsafe Control Actions

From Table 21, the set of potential causes of an unsafe control action are as follows:

1 standards, requirements, plant design basis documents and/or any information required for review of a safety factor area either does not exist, is not current, is missing or is incorrect.

2 standards and/or requirements do not match the safety factor area as implemented"

3 no definition of the business process to conduct periodic safety reviews

4 decision makers not adequately trained in requirements for performing periodic safety reviews
5 inadequate budget allocated to support PSR
6 inadequate staffing of personnel with the required skills for PSR
7 responsibility for initiating a PSR not defined
8 inadequate understanding by decision makers on the scope and personnel requirements necessary to conduct an effective PSR
9 inadequate priority given to conducting the PSR
10 perception that the current state of all safety factors is acceptable and hence scheduling a PSR is a low priority
11 lack of understanding on the frequency for conducting a PSR
12 priority and/or expectations for the performance of PSR not clearly communicated
13 responsibilities for performing PSR in each safety factor area is not clearly defined and/or communicated
14 lack of establishing effective performance measures that reflect the current state of each safety factor area
15 need to conduct PSR is not communicated in a timely manner to allow the needs to be incorporated into business plans
16 hiring of staff with the appropriate knowledge and skills results in delays to performance of the PSR
17 human error
18 organizations and personnel assigned to perform the PSR do not have the necessary skills and knowledge
19 PSR findings and recommendations not communicated to requesters in a timely manner

Appendix 6 lists the above causes and then identifies design features to deal with each cause. The design features are based on the IAEA principles and also other typical design features used to deal with each cause.

The summary of the resulting design features is as follows:

Safety Management

- Establish a safety management system that ensuring the continuing safety of the plant design

- Establishment of a set of programs necessary to achieve and maintain safety along with the establishment of an effective management system for the programs
- Expectations that the safety management system be developed, applied and continuously improved shall be established
- The safety management system shall be integrated into the overall management system
- A complete set of operating limits and conditions are documented and consistent with design assumptions and intent
- comprehensive set of design basis documentation
- comprehensive set of operating history documentation
- comprehensive set of plant design documentation for all safety related structures, systems and components
- comprehensive set of standards and requirements established necessary to comply with all regulatory requirements
- Establishment of clear expectations on the documentation, revisions control and communication of the safety management system
- Establishment of controls over the configuration of the physical plant and its design
- Clear responsibility for the safety of the plant within the operating organization's management system
- Establishment of governance that focuses on optimizing safety by keeping radiation risks as low as reasonably achievable

Leadership

- Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety
- Clearly defined responsibilities for all managers to advocate and support a safety culture
- Designate an individual to be responsible for the safety of the plant design
- Safety policies establishing the priority for safety and the standards to be met for all safety related activities
- Written communication shall be preferred and spoken communication shall be minimized. If spoken communication is used, attention shall be given to ensuring that spoken instructions are clearly understood.
- During the operation and maintenance phase, the operating organization has the overriding responsibility for safety

- Responsibility for safety is in no way diluted by activities and responsibilities of designers, suppliers, constructors or regulators
- Possibility of human error is taken into account
- the possibility of human error is taken into account with appropriate checks and balances for all PSR tasks
- clear documentation of need for PSR and its priority is established as part of business planning
- need for periodic safety reviews is included in business planning process
- clear expectations on the need for a periodic safety review
- clear procedures for the conduct of periodic safety reviews
- clear responsibility is established for the initiation of periodic safety reviews
- decision maker for initiating PSR clearly communicates to each organization assigned responsibility for a portion of the PSR
- decision makers for initiating periodic safety reviews demonstrate a safety culture by prioritizing PSR scheduling appropriately

Competencies

- Establishment of a program to establish the necessary competencies required within the operating organization and the development and training program to maintain the required competencies
- Establishment of a training program that ensures that personnel assigned to safety related tasks have the necessary qualifications and competencies
- Personnel involved with safety related activities have the competencies necessary to perform their duties
- A training program is established to ensure that personnel assigned safety related activities are knowledgeable of the operating limits and conditions
- Governance for assigning personnel to safety related tasks includes confirmation that the personnel have the necessary qualifications and competencies
- Programs to educate personnel their role in achieving and maintaining safety
- Programs to communicate and train personnel in the safety policies
- Clear definitions for the qualifications and competencies of personnel assigned to safety related activities are documented.
- business planning includes identification of staff levels of qualified staff able to conduct PSR activities in all required areas

- definition of qualifications for decision makers for periodic safety review initiation includes requirements on periodic safety reviews
- training established and delivered to decision makers for periodic safety review initiation

Assessments and Audits

- Expectation that safety goals are periodically reviewed against organizational strategies and plans are established
- Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner.
- Continuous improvement program focused on operational safety
- A continuous improvement program is established that revises operating limits and conditions based on operating experience
- Operating experience and research relevant to safety is used to identify areas for improvement to safety
- Establish an audit and review program to ensure that the safety management program has been effectively implemented and continuously improved over time
- Establish the organization responsible for audit and review to have sufficient authority and organizational independence to be able to identify problems, to recommend solutions and to verify that solutions have been effectively implemented.
- Self-assessment used to evaluate effectiveness of processes against pre-established expectations
- Peer review used to identify areas for improvement
- Ongoing, independent safety reviews in place
- expectations established for the documentation of all PSR findings and recommendations and the schedule for their production and communication
- performance measures are defined and measured for all safety factor areas supporting the PSR

12 ASSESSMENT OF EXAMPLE

This chapter assesses the degree to which the example in Chapter 11 addresses the weaknesses in nuclear current practices listed in section 9.3. For each recommendation assessment criteria are established (section 12.1), an assessment is performed using the criteria (section 12.2) and then conclusions are made on the degree to which the example demonstrates the SEE approach's ability to address the recommendation (section 12.3).

12.1 Assessment Criteria

As documented in Chapter 9, there were 14 recommendations related to nuclear safety from the IAEA report on Fukushima. There were also three recommendations related to emergency preparedness, management of radiological consequences and planning for post-accident recovery for a total of 17 recommendations. The seventeen recommendations were:

1. The assessment of natural hazards needs to be sufficiently conservative
2. The safety of NPPs needs to be re-evaluated on a periodic basis to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly
3. The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on an NPP. The assessment of natural hazards also needs to consider their effects on multiple units at an NPP.
4. Operating experience programmes need to include experience from both national and international sources. Safety improvements identified through operating experience programmes need to be implemented promptly. The use of operating experience needs to be evaluated periodically and independently.
5. The defence in depth concept remains valid, but implementation of the concept needs to be strengthened at all levels by adequate independence, redundancy, diversity and protection against internal and external hazards.

There is a need to focus not only on accident prevention, but also on improving mitigation measures.

6. Instrumentation and control systems that are necessary during beyond design basis accidents need to remain operable in order to monitor essential plant safety parameters and to facilitate plant operations.

7. Robust and reliable cooling systems that can function for both design basis and beyond design basis conditions need to be provided for the removal of residual heat.

8. There is a need to ensure a reliable confinement function for beyond design basis accidents to prevent significant release of radioactive material to the environment.

9. Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a plant to withstand applicable beyond design basis accidents and to provide a high degree of confidence in the robustness of the plant design.

10. Accident management provisions need to be comprehensive, well designed and up to date. They need to be derived on the basis of a comprehensive set of initiating events and plant conditions and also need to provide for accidents that affect several units at a multi-unit plant.

11. Training, exercises and drills need to include postulated severe accident conditions to ensure that operators are as well prepared as possible. They need to include the simulated use of actual equipment that would be deployed in the management of a severe accident.

12. In order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body is independent and possesses legal authority, technical competence and a strong safety culture.

13. In order to promote and strengthen safety culture, individuals and organizations need to continuously challenge or re-examine the prevailing assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety.

14. A systemic approach to safety needs to consider the interactions between human, organizational and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations.

15. Emergency preparedness and response needs to be strengthened

16. Improve monitoring and management of radiological consequences

17. Planning for post-accident recovery needs to be implemented

Below, for each of the 17 recommendations a set of criteria are identified that should be true of the SEE example if it addresses the recommendation. The criteria were identified by reviewing the details of each recommendation and then identifying criteria that would reflect the successful implementation of the detailed recommendations. The IAEA principles in Appendix 3 were also reviewed to identify criteria that are applicable to each detailed recommendation.

1) The assessment of natural hazards needs to be sufficiently conservative

- Compliance with appropriate codes and standards
- Conservative design, construction and testing practices commensurate with safety objectives
- Design margins established to account for unanticipated failures.
- Designate an individual to be responsible for the safety of the plant design
- Effective and robust design process
- Effective and robust V&V
- hazard analysis takes into account complex scenarios and apply conservative assumptions, especially with events of very low frequency
- assumptions upon which the safety analysis is based should be validated by actual operating experience
- corrective actions required as a result of change to assumptions should be implemented in a timely manner
- natural hazards are included in scope of hazard analysis
- thresholds for determining whether natural hazards are included as design basis events or beyond design basis events are "sufficiently conservative"
- special attention is paid to uncertainties associated with maximum magnitude earthquakes

2) The safety of NPPs needs to be re-evaluated on a periodic basis to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly

- Establish a safety management system that ensuring the continuing safety of the plant design.

- Establishment of a safety management system that takes into account the safety significance of changes
- Establishment of a set of programs necessary to achieve and maintain safety along with the establishment of an effective management system for the programs
- Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner.
- Operating experience from the design, construction and operation of similar plants shall be taken into account.
- Establish a program to investigate events with significant implications for safety and take effective actions to avoid reoccurrence of the events.
- Effective change control process to implement changes in a timely manner
- Effective use of OPEX to identify needed changes
- periodic safety reviews conducted every 10 years
- periodic safety reviews take as input operating experience from other plants and advances in research
- recommendations and corrective actions from the periodic safety reviews are given adequate priority to be promptly implemented"
- standards used as input to a periodic safety review should be current and updated within a reasonable period
- the design should effectively address flooding hazards
- regulators require a continuous safety improvement process
- regulatory body is required to review and approve the safety demonstration
- modifications that may impact safety require regulatory review and approval
- emergency drills and exercises take due account of harsh, complex and unexpected conditions
- periodic, independent review performed of the effectiveness of the operating experience program
- assessment of new safety issues is performed in a timely manner
- corrective actions, both interim compensator actions and final corrective actions, are implemented in a timely manner
- approval of design improvements from a periodic safety review should be based on objective, risk informed decision making

3) **The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on an NPP. The assessment of natural hazards also needs to consider their effects on multiple units at an NPP.**
   - Compliance with appropriate codes and standards
   - Conservative design, construction and testing practices commensurate with safety objectives
   - Design margins established to account for unanticipated failures.
   - Designate an individual to be responsible for the safety of the plant design
   - Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.
   - Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents
   - hazard analysis takes into account complex scenarios involving multiple external hazards and possibly multiple NPPs

4) **Operating experience programmes need to include experience from both national and international sources. Safety improvements identified through operating experience programmes need to be implemented promptly. The use of operating experience needs to be evaluated periodically and independently.**
   - Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner.
   - Operating experience from the design, construction and operation of similar plants shall be taken into account.
   - Establish a program to investigate events with significant implications for safety and take effective actions to avoid reoccurence of the events.
   - assessment of operating experience takes into account sensitivity of risk to small changes to initiating events and conditions
   - decision making within the management system makes nuclear safety an overriding priority

5) **The defence in depth concept remains valid, but implementation of the concept needs to be strengthened at all levels by adequate independence, redundancy, diversity and protection against internal and external hazards. There is a need to focus not only on accident prevention, but also on improving mitigation measures.**

- Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.
- Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents
- Proven methods of manufacturing and construction
- Quality assurance applied to ensure with high level of confidence that safety requirements and objectives are met
- The design of items important to safety shall take into account the attributes of manufacturability, constructability and installabilty to ensure that the probability of introduction of undetected errors is commensurate with the level of risk of errors.
- Reliability targets are assigned to safety systems or functions. The targets are established on the basis of the safety objectives and are consistent with the roles of the systems or functions in different accident sequences. Provision is made for testing and inspection of components and systems for which reliability targets have been set.
- Technical specifications for items important to safety shall be developed using appropriate methods that result in complete and correct specifications of safety requirements.
- the approach to plant design systematically addresses flooding hazards by trying to eliminate, control or mitigate the causes of the flooding hazards
- design takes into account and addresses failures of safety functions up to DID level 3 functions

6) **Instrumentation and control systems that are necessary during beyond design basis accidents need to remain operable in order to monitor essential plant safety parameters and to facilitate plant operations.**
   - design provides for functioning critical instrumentation in all scenarios leading to severe accidents

7) **Robust and reliable cooling systems that can function for both design basis and beyond design basis conditions need to be provided for the removal of residual heat.**

- provisions made for alternate means of removal of decay heat should permanently installed equipment not be operable

8) **There is a need to ensure a reliable confinement function for beyond design basis accidents to prevent significant release of radioactive material to the environment.**
   - confinement function takes into account beyond design basis accidents

9) **Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a plant to withstand applicable beyond design basis accidents and to provide a high degree of confidence in the robustness of the plant design.**
   - deterministic and probabilistic beyond design basis safety analyses need to be comprehensive and take into account both internal and external events, including internal flooding and external hazards such as seismic events and flooding.
   - low probability numbers within a PSA are reviewed and confirmed
   - safety demonstration needs to take into account human, technological and organizational aspects and how their interactions impact safety

10) **Accident management provisions need to be comprehensive, well designed and up to date. They need to be derived on the basis of a comprehensive set of initiating events and plant conditions and also need to provide for accidents that affect several units at a multi-unit plant.**
   - emergency planning takes into account design basis events, including tsunamis
   - emergency planning procedures take into account the period of time before, during and after a tsunami
   - safety functions required to support DiD levels 4 are independent from those of levels 1, 2 and 3, and do not have any common mode failure modes
   - Interconnections between units need to be designed to prevent an accident from migrating from one unit to another.
   - Accident management provisions need to be clear, comprehensive and well designed.
   - Provisions for the proper management of hydrogen need to be considered.

11) **Training, exercises and drills need to include postulated severe accident conditions to ensure that operators are as well prepared as possible. They need to include the simulated use of actual equipment that would be deployed in the management of a severe accident.**
    - Personnel need to be trained to manage severe plant conditions (Level 4). This training needs to include consideration of the extreme environmental conditions which may prevail during a severe accident.
    - Training and exercises need to be based on realistic severe accident conditions.

12) **In order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body is independent and possesses legal authority, technical competence and a strong safety culture.**
    - Regulatory bodies need to ensure that adequate AM provisions are in place, taking into account severely damaged infrastructures and long duration accidents.
    - implementation of the regulatory function is effective and avoids omissions or duplications that may jeopardize safety
    - regulator has qualified, independent personnel and strong legislative authority
    - regulator acknowledges its role within the national nuclear system
    - regulator acknowledges its impact on the nuclear industry's safety culture
    - regulatory body confirms that licensees are taking appropriate actions in response to operating experience

13) **In order to promote and strengthen safety culture, individuals and organizations need to continuously challenge or re-examine the prevailing assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety.**
    - The operating organization shall encourage plant personnel to have a questioning attitude and to make appropriate and conservative decisions, so as to minimize risk and to maintain the plant in a safe condition.
    - the approach to nuclear safety takes into account that the unexpected can occur
    - strong safety culture

- ongoing public dialogue is carried out in a transparent manner

14) **A systemic approach to safety needs to consider the interactions between human, organizational and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations.**
    - approach to safety takes into account results of research on complex sociotechnical systems

15) **Emergency preparedness and response needs to be strengthened**
    - Utilizes an all-hazards approach in developing preparedness and response arrangements
    - Develops an emergency classification system on the basis of observable conditions and measurable criteria (emergency action levels) and initiation of predetermined urgent protective actions for the public (in the predefined zones) promptly following the classification of the emergency by the operator
    - Establishes emergency zones for the full range of possible emergencies, including those of low probability
    - Establishes arrangements for the implementation of protective actions within the emergency zones and beyond, as required
    - Sets national criteria for decisions on public protective actions (evacuation, sheltering, iodine thyroid blocking, relocation, restriction of food and drinking water consumption and distribution, public monitoring and decontamination) in terms of doses and measurable quantities (operational intervention levels), taking account of a range of factors (such as financial and social aspects)
    - Makes arrangements for carrying out radiation monitoring and environmental sampling and assessment in order to identify new hazards promptly and to refine the strategy for response
    - Identifies, at the preparedness stage, special population groups within emergency zones (e.g. disabled persons, hospital patients) for whom specific arrangements need to be made
    - Establishes arrangements for emergency workers, including setting the dose criteria for different types of tasks, designating emergency workers and ensuring their protection, establishing guidance for managing, controlling and recording their doses, and providing specialized protective equipment, procedures and training

- Plans for the transition from the emergency phase to long term recovery operations and resumption of normal social and economic activities, including clear allocation of responsibilities, sharing and transferring information, assessing consequences, establishing formal processes to decide on withdrawal of restrictions and other arrangements imposed during the emergency, setting relevant principles and criteria and consulting the public
- Clearly assigns roles, responsibilities and authorities for emergency preparedness and response at all levels as part of emergency plans
- Establishes organizational relationships and interfaces among operating and response organizations and preparing operational protocols to coordinate the emergency response at all levels
- Develops and coordinating emergency plans and procedures at all levels on the basis of assessed hazards
- Prepares for logistical support through provision of tools, instruments, supplies, equipment, communication systems, specific functional facilities and documentation, including planning for operability and usability of these items and facilities under postulated radiological, working and environmental conditions in the emergency response
- Plans for and conducting of training, drills and exercises; and
- Establishes a quality assurance programme to ensure that all the supplies, equipment, communication systems, facilities and documentation, etc., are kept continuously up to date, available and functional for use in an emergency.

16) Improve monitoring and management of radiological consequences

- In case of an accidental release of radioactive substances to the environment, the prompt quantification and characterization of the amount and composition of the release is needed. For significant releases, a comprehensive and coordinated programme of long term environmental monitoring is necessary to determine the nature and extent of the radiological impact on the environment at the local, regional and global levels.
- Relevant international bodies need to develop explanations of the principles and criteria for radiation protection that are understandable for non-specialists in order to make their application clearer for decision makers and the public. As some protracted protection measures were disruptive for the affected people, a better communication strategy is

needed to convey the justification for such measures and actions to all stakeholders, including the public.

- Conservative decisions related to specific activity and activity concentrations in consumer products and deposition activity led to extended restrictions and associated difficulties. In a prolonged exposure situation, consistency among international standards, and between international and national standards, is beneficial, particularly those associated with drinking water, food, non-edible consumer products and deposition activity on land.
- Personal radiation monitoring of representative groups of members of the public provides invaluable information for reliable estimates of radiation doses and needs to be used together with environmental measurements and appropriate dose estimation models for assessing public dose.
- While dairy products were not the main pathway for the ingestion of radioiodine in Japan, it is clear that the most important method of limiting thyroid doses, especially to children, is to restrict the consumption of fresh milk from grazing cows.
- A robust system is necessary for monitoring and recording occupational radiation doses, via all relevant pathways, particularly those due to internal exposure that may be incurred by workers during severe accident management activities. It is essential that suitable and sufficient personal protective equipment be available for limiting the exposure of workers during emergency response activities and that workers be sufficiently trained in its use.
- The risks of radiation exposure and the attribution of health effects to radiation need to be clearly presented to stakeholders, making it unambiguous that any increases in the occurrence of health effects in populations are not attributable to exposure to radiation if levels of exposure are similar to the global average background levels of radiation.
- After a nuclear accident, health surveys are very important and useful, but should not be interpreted as epidemiological studies. The results of such health surveys are intended to provide information to support medical assistance to the affected population.
- There is a need for radiological protection guidance to address the psychological consequences to members of the affected populations in the aftermath of radiological accidents. A Task Group of the ICRP has recommended that “strategies for mitigating the serious psychological consequences arising from radiological accidents be sought”

- Factual information on radiation effects needs to be communicated in an understandable and timely manner to individuals in affected areas in order to enhance their understanding of protection strategies, to alleviate their concerns and support their own protection initiatives.
- During any emergency phase, the focus has to be on protecting people. Doses to the biota cannot be controlled and could be potentially significant on an individual basis. Knowledge of the impacts of radiation exposure on non-human biota needs to be strengthened by improving the assessment methodology and understanding of radiation induced effects on biota populations and ecosystems. Following a large release of radionuclides to the environment, an integrated perspective needs to be adopted to ensure sustainability of agriculture, forestry, fishery and tourism, and of the use of natural resources.

17) Planning for post-accident recovery needs to be implemented

- Pre-accident planning for post-accident recovery is necessary to improve decision making under pressure in the immediate post-accident situation. National strategies and measures for post-accident recovery need to be prepared in advance in order to enable an effective and appropriate overall recovery programme to be put in place in case of a nuclear accident. These strategies and measures need to include the establishment of a legal and regulatory framework; generic remediation strategies and criteria for residual radiation doses and contamination levels; a plan for stabilization and decommissioning of damaged nuclear facilities; and a generic strategy for managing large quantities of contaminated material and radioactive waste.
- Remediation strategies need to take account of the effectiveness and feasibility of individual measures and the amount of contaminated material that will be generated in the remediation process.
- As part of the remediation strategy, the implementation of rigorous testing of and controls on food is necessary to prevent or minimize ingestion doses.
- Further international guidance is needed on the practical application of safety standards for radiation protection in post-accident recovery situations.
- Following an accident, a strategic plan for maintaining long term stable conditions and for the decommissioning of accident damaged facilities is

essential for on-site recovery. The plan needs to be flexible and readily adaptable to changing conditions and new information.

- Retrieving damaged fuel and characterizing and removing fuel debris require solutions that are specific to the accident, and special methods and tools may need to be developed.
- National strategies and measures for post-accident recovery need to include the development of a generic strategy for managing contaminated liquid and solid material and radioactive waste, supported by generic safety assessments for discharge, storage and disposal.
- It is necessary to recognize the socioeconomic consequences of any nuclear accident and of the subsequent protective actions, and to develop revitalization and reconstruction projects that address issues such as reconstruction of infrastructure, community revitalization and compensation.
- Support by stakeholders is essential for all aspects of post-accident recovery. In particular, engagement of the affected population in the decision making processes is necessary for the success, acceptability and effectiveness of the recovery and for the revitalization of communities. An effective recovery programme requires the trust and the involvement of the affected population. Confidence in the implementation of recovery measures has to be built through processes of dialogue, the provision of consistent, clear and timely information, and support to the affected population.

12.2 Assessment of Whether Fukushima Recommendations are Addressed by SEE Approach

This Section assesses the SEE example in Section 11.2 using the criteria in the previous Section to determine the degree to which the example addresses the recommendations from the Fukushima accident. Each individual criteria is shown as being:

- satisfied,
- not-satisfied or
- not applicable due to limited scope of example (NA).

A summary of the degree to which each recommendation is addressed is then made. Section 12.3 then provides conclusions based on this assessment.

1) The assessment of natural hazards needs to be sufficiently conservative

Criteria	Satisfaction of Criteria
Compliance with appropriate codes and standards	Satisfied
Conservative design, construction and testing practices commensurate with safety objectives	Satisfied
Design margins established to account for unanticipated failures.	Satisfied
Designate an individual to be responsible for the safety of the plant design	Satisfied
Effective and robust design process	Satisfied
Effective and robust V&V	Satisfied
Hazard analysis takes into account complex scenarios and apply conservative assumptions, especially with events of very low frequency	Satisfied
Assumptions upon which the safety analysis is based should be validated by actual operating experience	Satisfied
Corrective actions required as a result of change to assumptions should be implemented in a timely manner	Satisfied
Natural hazards are included in scope of hazard analysis	NA
Thresholds for determining whether natural hazards are included as design basis events or beyond design basis events are "sufficiently conservative"	NA
Special attention is paid to uncertainties associated with maximum magnitude earthquakes	NA

The results of the example demonstrate conservatism in design and operation of the plant. The scope of the example did not provide for specific demonstration of the assessment of natural hazards.

The IAEA principles establish the need for a safety program to ensure continuing safety of the plant over its lifetime, and the need for ongoing review of safety based on operating experience and research results.

The approach to hazard analysis in the SEE approach is not fundamentally probabilistic in nature and hence starts with the assumption that hazards will occur making it more conservative as compared to traditional nuclear safety analysis (which will ignore very low probability events).

2) The safety of NPPs needs to be re-evaluated on a periodic basis to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly

Criteria	Satisfaction of Criteria
Establish a safety management system that ensuring the continuing safety of the plant design.	Satisfied
Establishment of a safety management system that takes into account the safety significance of changes	Satisfied
Establishment of a set of programs necessary to achieve and maintain safety along with the establishment of an effective management system for the programs	Satisfied
Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner.	Satisfied
Operating experience from the design, construction and operation of similar plants shall be taken into account.	Satisfied
Establish a program to investigate events with significant implications for safety and take effective actions to avoid reoccurrence of the events.	Satisfied

Criteria	Satisfaction of Criteria
Effective change control process to implement changes in a timely manner	Satisfied
Effective use of OPEX to identify needed changes	Satisfied
Periodic safety reviews conducted every 10 years	Satisfied
Periodic safety reviews take as input operating experience from other plants and advances in research	Satisfied
Recommendations and corrective actions from the periodic safety reviews are given adequate priority to be promptly implemented	Satisfied
Standards used as input to a periodic safety review should be current and updated within a reasonable period	Not Satisfied
The design should effectively address flooding hazards	NA
Regulators require a continuous safety improvement process	Not Satisfied
Regulatory body is required to review and approve the safety demonstration	Not Satisfied
Modifications that may impact safety require regulatory review and approval	Not Satisfied
Emergency drills and exercises take due account of harsh, complex and unexpected conditions	NA
Periodic, independent review performed of the effectiveness of the operating experience program	Satisfied
Assessment of new safety issues is performed in a timely manner	Not Satisfied
Corrective actions, both interim compensator actions and final corrective actions, are implemented in a timely manner	Satisfied

Criteria	Satisfaction of Criteria
Approval of design improvements from a periodic safety review should be based on objective, risk informed decision making	Not Satisfied

The example did demonstrate that safety needed to be re-evaluated on a periodic basis. Some of the assessment criteria related to regulatory interactions related to re-evaluation of safety were not demonstrated since the example did not deal directly with regulatory interactions.

The IAEA principles clearly establish the need for ongoing review of safety and implementation of corrective actions. The SEE approach clearly establishes the need for processes for performance monitoring and continuous improvement.

3) The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on an NPP. The assessment of natural hazards also needs to consider their effects on multiple units at an NPP.

Criteria	Satisfaction of Criteria
Compliance with appropriate codes and standards	Satisfied
Conservative design, construction and testing practices commensurate with safety objectives	Satisfied
Design margins established to account for unanticipated failures.	Satisfied
Designate an individual to be responsible for the safety of the plant design	Satisfied
Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.	Satisfied
Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents	Satisfied

Criteria	Satisfaction of Criteria
Hazard analysis takes into account complex scenarios involving multiple external hazards and possibly multiple npps	Satisfied

The example demonstrated the SEE approach's ability to deal with combinations of events. Handling of complex scenarios and very low frequency events is a deficiency in current standards and practices. STPA hazard analysis inherently addresses all means by which hazardous states can occur and hence addresses both complex scenarios and very low probability events.

4) Operating experience programmes need to include experience from both national and international sources. Safety improvements identified through operating experience programmes need to be implemented promptly. The use of operating experience needs to be evaluated periodically and independently.

Criteria	Satisfaction of Criteria
Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner.	Satisfied
Operating experience from the design, construction and operation of similar plants shall be taken into account.	Satisfied
Establish a program to investigate events with significant implications for safety and take effective actions to avoid reoccurrence of the events.	Satisfied
Assessment of operating experience takes into account sensitivity of risk to small changes to initiating events and conditions	Satisfied
Decision making within the management system makes nuclear safety an overriding priority	Satisfied

The example demonstrated that operating history is used to identify and implement improvements to safety over the life of the plant. IAEA principles establish the need for ongoing review of safety based on operating experience and research results. STPA analysis is not fundamentally probabilistic in nature and hence starts with assumption that hazards will occur making it more conservative as compared to traditional nuclear safety analysis (which will ignore very low probability events). SEE clearly establishes the need for processes for performance monitoring and continuous improvement.

5) The defence in depth concept remains valid, but implementation of the concept needs to be strengthened at all levels by adequate independence, redundancy, diversity and protection against internal and external hazards. There is a need to focus not only on accident prevention, but also on improving mitigation measures.

Criteria	Satisfaction of Criteria
Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.	Satisfied
Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents	Satisfied
Proven methods of manufacturing and construction	Satisfied
Quality assurance applied to ensure with high level of confidence that safety requirements and objectives are met	Satisfied
The design of items important to safety shall take into account the attributes of manufacturability, constructability and installabilty to ensure that the probability of introduction of undetected errors is commensurate with the level of risk of errors.	Satisfied
Reliability targets are assigned to safety systems or functions. The targets are established on the basis of the safety objectives and are consistent with the roles of the systems or functions in different	Satisfied

Criteria	Satisfaction of Criteria
accident sequences. Provision is made for testing and inspection of components and systems for which reliability targets have been set.	
Technical specifications for items important to safety shall be developed using appropriate methods that result in complete and correct specifications of safety requirements.	Satisfied
The approach to plant design systematically addresses flooding hazards by trying to eliminate, control or mitigate the causes of the flooding hazards	NA
Design takes into account and addresses failures of safety functions up to DID level 3 functions	Not Satisfied

The example demonstrated that the defence in depth is implemented rigorously. IAEA principles establish the DiD requirements clearly. TEPCO was non-compliant with the key requirements for independence, redundancy, diversity and protection from hazards associated with flooding from a large tsunami. The traditional approach to nuclear safety analysis may make non-conservative assumptions (such as the maximum height of a tsunami) and the need to address very low frequency events (like a large tsunami) which could lead to a situation where the DiD strategy is ineffective. STPA inherently is not based on a probabilistic approach and hence will not have the same weaknesses as the traditional approach.

6) Instrumentation and control systems that are necessary during beyond design basis accidents need to remain operable in order to monitor essential plant safety parameters and to facilitate plant operations.

Criteria	Satisfaction of Criteria
Design provides for functioning critical instrumentation in all scenarios leading to severe accidents	NA

The example scope did not directly address systems required after a beyond design basis event. The traditional approach to nuclear safety analysis may make non-conservative assumptions (such as the maximum height of a tsunami) and the need to address very low frequency events (like a large tsunami) which could lead to a situation where the DiD strategy was ineffective. STPA inherently is not based on a probabilistic approach and hence will not have the same weaknesses as the traditional approach. IAEA principles establish the DiD requirements clearly. TEPCO was non-compliant with the key requirements for independence, redundancy, diversity and protection from hazards associated with flooding from a large tsunami. Compliance with DiD requirements coupled with a non-probabilistic approach to hazard analysis will ensure that critical instrumentation and control systems will remain operable during a beyond design basis event.

7) Robust and reliable cooling systems that can function for both design basis and beyond design basis conditions need to be provided for the removal of residual heat.

Criteria	Satisfaction of Criteria
Provisions made for alternate means of removal of decay heat should permanently installed equipment not be operable	NA

The scope of the example did not allow for demonstration of the reliability of the cooling systems. The traditional approach to nuclear safety analysis may make non-conservative assumptions (such as the maximum height of a tsunami) and the need to address very low frequency events (like a large tsunami) which could lead to a situation where the DiD strategy was ineffective. STPA inherently is not based on a probabilistic approach and hence will not have the same weaknesses as the traditional approach. Compliance with DiD requirements coupled with a non-probabilistic approach to hazard analysis will ensure that robust and reliable cooling is provided during a design basis and beyond design basis event.

8) There is a need to ensure a reliable confinement function for beyond design basis accidents to prevent significant release of radioactive material to the environment.

Criteria	Satisfaction of Criteria
Confinement function takes into account beyond design basis accidents	NA

The scope of the example did not deal with the confinement function and hence did not demonstrate this criterion. The traditional approach to nuclear safety analysis may make non-conservative assumptions (such as the maximum height of a tsunami) and the need to address very low frequency events (like a large tsunami) which could lead to a situation where the DiD strategy was ineffective. STPA inherently is not based on a probabilistic approach and hence will not have the same weaknesses as the traditional approach. Compliance with DiD requirements coupled with a non-probabilistic approach to hazard analysis will ensure that robust and reliable cooling is provided during a design basis and beyond design basis event.

9) Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a plant to withstand applicable beyond design basis accidents and to provide a high degree of confidence in the robustness of the plant design.

Criteria	Satisfaction of Criteria
Deterministic and probabilistic beyond design basis safety analyses need to be comprehensive and take into account both internal and external events, including internal flooding and external hazards such as seismic events and flooding.	Satisfied
Low probability numbers within a PSA are reviewed and confirmed	Satisfied
Safety demonstration needs to take into account human, technological and organizational aspects and how their interactions impact safety	Satisfied

The example did not demonstrate a comprehensive probabilistic safety analysis since the SEE approach is not based on a probabilistic approach. It will take into account a broader scope of causes of hazards since it takes into account low

probability events that would not be considered in a traditional safety analysis approach. STPA provides an alternative to performing a "more comprehensive" PSA to address complex scenarios and very low frequency events. The SEE approach explicitly addresses interactions between human, technological and organizational aspects.

10) Accident management provisions need to be comprehensive, well designed and up to date. They need to be derived on the basis of a comprehensive set of initiating events and plant conditions and also need to provide for accidents that affect several units at a multi-unit plant.

Criteria	Satisfaction of Criteria
Emergency planning takes into account design basis events, including tsunamis	NA
Emergency planning procedures take into account the period of time before, during and after a tsunami	NA
Safety functions required to support did levels 4 are independent from those of levels 1, 2 and 3, and do not have any common mode failure modes	Not Satisfied
Interconnections between units need to be designed to prevent an accident from migrating from one unit to another.	Not Satisfied
Accident management provisions need to be clear, comprehensive and well designed.	NA
Provisions for the proper management of hydrogen need to be considered.	NA

The scope of the example does not address accident management provisions. IAEA requirements establish the need for accident management provisions. Weaknesses at Fukushima were with respect to the non-conservative assumptions which resulted in inadequate scenarios against which to plan the accident management provisions.

11) Training, exercises and drills need to include postulated severe accident conditions to ensure that operators are as well prepared as possible. They need to include the simulated use of actual equipment that would be deployed in the management of a severe accident.

Criteria	Satisfaction of Criteria
Personnel need to be trained to manage severe plant conditions (Level 4). This training needs to include consideration of the extreme environmental conditions which may prevail during a severe accident.	NA
Training and exercises need to be based on realistic severe accident conditions.	NA

The scope of the example does not address accident management provisions. IAEA requirements establish the need for accident management provisions. Weaknesses at Fukushima were with respect to the non-conservative assumptions which resulted in inadequate scenarios against which to plan the accident management provisions. The organizational design approach of SEE will contribute to improving performance in this area.

12) In order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body is independent and possesses legal authority, technical competence and a strong safety culture.

Criteria	Satisfaction of Criteria
Regulatory bodies need to ensure that adequate AM provisions are in place, taking into account severely damaged infrastructures and long duration accidents.	NA
Implementation of the regulatory function is effective and avoids omissions or duplications that may jeopardize safety	Satisfied
Regulator has qualified, independent personnel and strong legislative authority	Satisfied

Criteria	Satisfaction of Criteria
Regulator acknowledges its role within the national nuclear system	Not Satisfied
Regulator acknowledges its impact on the nuclear industry's safety culture	Not Satisfied
Regulatory body confirms that licensees are taking appropriate actions in response to operating experience	Not Satisfied

The scope of the example did not deal directly with regulatory issues and hence did not demonstrate this criterion very well. IAEA requirements for the regulatory function are established. The main problem at Fukushima was the common perspective, both by the utility and the regulator, that low probability events did not need to be dealt with. The SEE approach utilizes an improved hazard analysis technique that is not dependent on probabilities and uses explicit modeling and hazard analysis of the regulatory interface.

13) In order to promote and strengthen safety culture, individuals and organizations need to continuously challenge or re-examine the prevailing assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety.

Criteria	Satisfaction of Criteria
The operating organization shall encourage plant personnel to have a questioning attitude and to make appropriate and conservative decisions, so as to minimize risk and to maintain the plant in a safe condition.	Satisfied
The approach to nuclear safety takes into account that the unexpected can occur	Satisfied
Strong safety culture	Satisfied
Ongoing public dialogue is carried out in a transparent manner	NA

The example demonstrated the implementation of a strong safety culture. IAEA requirements establish the need for a strong safety culture. SEE's safety control structure modeling of governance results in a more direct assessment of safety culture and the pre-requisite design features necessary to achieve it.

14) A systemic approach to safety needs to consider the interactions between human, organizational and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations.

Criteria	Satisfaction of Criteria
Approach to safety takes into account results of research on complex sociotechnical systems	Satisfied

The example demonstrated the considerations of interactions between humans, organizational and technical factors. IAEA principles establish requirements on human, organizational and technical factors but do not have requirements on their interactions. SEE models and analyzes all these aspects including their interactions that may result in hazardous states.

15) Emergency preparedness and response needs to be strengthened

Criteria	Satisfaction of Criteria
All criteria	NA

The scope of the example did not deal with emergency preparedness and response needs.

16) Improve monitoring and management of radiological consequences

Criteria	Satisfaction of Criteria
All criteria	NA

The scope of the example did not deal with management of radiological consequences.

17) Planning for post-accident recovery needs to be implemented

Criteria	Satisfaction of Criteria
All criteria	NA

The scope of the example did not deal with planning for post-accident recovery.

12.3 Conclusions from Assessment

Table 22 shows the weaknesses in current practice (from Section 9.3) and then shows how successful the SEE approach is in addressing these weaknesses, as compared with how successful IAEA best practice is in addressing the same weaknesses.

From the table it can be seen that there are three areas of weakness where the SEE approach performed better (numbers 3, 9 and 14). In fact, for those three weaknesses, the IAEA best practice did nothing to address the problem.

Weaknesses numbered 3 and 9 relate to the ability of safety analysis to comprehensively take into account combinations of events, either simultaneously or sequentially. Typical nuclear safety analysis is based on a deterministic safety analysis and a probabilistic safety analysis. Deterministic nuclear safety analysis takes into account two sets of events; design basis events and beyond design basis events. Design basis events do not include low probability events or combinations of events that can lead to accidents. Beyond design basis events do consider some combinations of events but exclude conditions that are considered extremely unlikely to arise.

Fukushima demonstrated this weakness in that a 15 meter tsunami was considered extremely unlikely to occur and hence was not adequately considered in the design of the plant. The SEE approach does not consider probabilities in its

hazard analysis and hence will identify design features to address causes of hazards even if they would be considered extremely unlikely to arise.

Weakness 14 relates to the need for a systemic approach to safety that deals with interactions between human, organizational and technical factors. The SEE approach deals with all these factors. Again, the IAEA best practice did not address this weakness.

No.	Weakness in Current Practice	Best Practice Coverage of Current Practice Weaknesses ✓ Fully / - Partial / X Not	SEE Approach Example Coverage of Weaknesses		
			P Fully / - Partial / X Not	Out of Scope of Example	
1	The assessment of natural hazards needs to be sufficiently conservative	-	✓	NA	
2	The safety of NPPs needs to be re-evaluated on a periodic basis to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly	-	-	NA	
3	The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on an NPP. The assessment of natural hazards also needs to consider their effects on multiple units at an NPP.	X	✓		
4	Operating experience programmes need to include experience from both national and international sources. Safety improvements identified through operating experience programmes need to be implemented promptly. The use of operating experience needs to be evaluated periodically and independently.	✓	✓		
5	The defence in depth concept remains valid, but implementation of the concept needs to be strengthened at all levels by adequate independence, redundancy, diversity and protection against internal and external hazards. There is a need to focus not only on accident prevention, but also on improving mitigation measures.	-	-	NA	
6	Instrumentation and control systems that are necessary during beyond design basis accidents need to remain operable in order to monitor essential plant safety parameters and to facilitate plant operations.	✓		NA	
7	Robust and reliable cooling systems that can function for both design basis and beyond design basis conditions need to be provided for the removal of residual heat.	-		NA	
8	There is a need to ensure a reliable confinement function for beyond design basis accidents to prevent significant release of radioactive material to the environment.	✓		NA	
9	Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a plant to withstand applicable beyond design basis accidents and to provide a high degree of confidence in the robustness of the plant design.	X	✓		
10	Accident management provisions need to be comprehensive, well designed and up to date. They need to be derived on the basis of a comprehensive set of initiating events and plant conditions and also need to provide for accidents that affect several units at a multi-unit plant.	✓	-	NA	
11	Training, exercises and drills need to include postulated severe accident conditions to ensure that operators are as well prepared as possible. They need to include the simulated use of actual equipment that would be deployed in the management of a severe accident.	✓		NA	
12	In order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body is independent and possesses legal authority, technical competence and a strong safety culture.	-	-	NA	
13	In order to promote and strengthen safety culture, individuals and organizations need to continuously challenge or re-examine the prevailing assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety.	-	✓	NA	
14	A systemic approach to safety needs to consider the interactions between human, organizational and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations.	X	✓		
15	Emergency preparedness and response needs to be strengthened	-		NA	
16	Improve monitoring and management of radiological consequences	-		NA	
17	Planning for post-accident recovery needs to be implemented	-		NA	

Table 22 - Coverage of Nuclear Practice Weaknesses by SEE Approach Example

Some of the key aspects of the SEE approach that were significant with respect to improving on nuclear practices were:

- STPA analysis is not fundamentally probabilistic in nature and hence starts with the assumption that hazards will occur making it more conservative as compared to traditional nuclear safety analysis (which will ignore very low probability events)

- STPA inherently addresses all means by which hazardous states can occur and hence addresses both complex scenarios and very low probability events

- STPA provides an alternative to performing a “more comprehensive” PSA to address complex scenarios and very low frequency events

- Traditional approaches to nuclear safety analysis may make non-conservative assumptions (such as the maximum height of a tsunami) and the need to address very low frequency events (like a large tsunami) which could lead to a situation where the Defense in Depth strategy was ineffective

- SEE models and analyzes all human, organizational and technical factors including their interactions that may result in hazardous states

13 CONCLUSIONS

Significant accidents are often related to the performance of a complex socio-technical system (enterprise). Methodical approaches to identify factors that lead to accidents and then take them into account during the design, operation, maintenance and evolution of the socio-technical system (enterprise) are not well defined and not consistently utilized in practice.

The main contribution of this thesis has been the definition and demonstration of a Safety Enterprise Engineering (SEE) approach to the design, operation, maintenance and evolution of enterprises in order to achieve safety goals. An example, based on practices in the nuclear industry, was used to demonstrate the effectiveness of the approach.

The definition of the SEE approach consists of the following steps:

- Definition of foundational concepts related to safety, (Chapter 4)
- Definition of the safety enterprise engineering process, (Chapter 5)
- Definition of the hazard analysis process applicable to enterprise engineering, (Chapter 6)
- Definition of a model of an enterprise to define the elements of the enterprise to be designed (Chapter 7) and
- Definition of principles that address typical classes of hazards by reviewing nuclear best practices and mapping them into the applicable portion of the enterprise design. (Chapter 8)

The demonstration of the SEE approach within the nuclear power industry consisted of the following steps:

- Use of the Fukushima Daiichi accident in 2011 to identify weaknesses with current practices within the nuclear industry, (Chapter 9)
- Use of IAEA best practices documents to identify weaknesses from Fukushima that are not well addressed by nuclear best practice, (Chapter 10) and
- Application of the SEE approach to a slice of safety related functionality of a typical CANDU nuclear utility to assess the degree to which the SEE approach addresses weaknesses in current and best practices within the nuclear industry. (Chapters 11 and 12)

The SEE approach was shown to improve on current and best practice in the nuclear power industry.

The SEE approach uses an integrated approach to engineering the entire enterprise as opposed to only engineering the dangerous technology for which the enterprise is responsible. The approach deals with the enterprise as a socio-technical system including the dangerous technology, people within the enterprise, the organization of people, the business processes used by the people and enterprise governance. The approach addresses lifecycle phases of design, construction, operation, maintenance and evolution of the enterprise.

The SEE approach is able to deal with the complexities of a socio-technical system. The approach deals with equipment failures, human performance errors and unintended interactions between system elements that can result in accidents. It is also able to deal with multiple, concurrent failures along with low probability events that can lead to accidents.

The use of a stepwise refinement approach aids in the establishment of high level principles important to safety in the early stages of design and flow them down to the detailed design level.

As a result of the Fukushima accident it was observed that "Current approaches for regulating nuclear plant safety, which traditionally have been based on deterministic concepts such as the design-basis accident, are clearly inadequate for preventing core-melt accidents and mitigating their consequences." [1] The recommendation for overcoming this shortcoming was to expand probabilistic risk assessment (PRA) to be more comprehensive. The disadvantages of this approach were observed in [1] to be:

- PRAs are expensive and can be time-consuming to produce and maintain.
- Extending the scope of PRAs will require additional technical expertise, especially in containment response analysis and offsite impacts. Obtaining this expertise could be difficult for industry and the USNRC,
- PRAs that have been performed generally do not adequately account for human error in design, construction, maintenance, and operation of nuclear plants or for intentional sabotage,
- The results of PRAs are limited by experts' ability to recognize all relevant phenomena, including potentially important external hazards, and by uncertainties and incompleteness of estimates of accident probabilities and consequences.

- The results of full-scope PRAs are also limited by the ability to validate phenomenological modeling of core damage and radioactive release as well as consequence modeling

The SEE approach can deal with multiple human and equipment failures since the hazard analysis of the safety-control-structure model identifies hazards even if they are the outcome of multiple failures without having to identify all the various means by which the hazard can occur.

The approach also avoids FMEA / FTA limitations with respect to the effort and ability of the analyst to identify and understand all multiple concurrent failure scenarios.

The safety-control-structure model includes modeling of roles of humans and therefore identifies potential hazardous actions taken by humans so that the hazards can be eliminated, controlled or mitigated

STPA analysis tends to not focus on probabilities of occurrence (only severity of consequences) and so will better address accidents resulting from low probability events.

SEE therefore is a more effective response to the observed shortcomings with current practice for achieving safety in the nuclear industry.

13.1 Contributions

The contributions of the research include:

- the definition of a holistic approach to achieving safety that spans the whole lifecycle of a system, and includes both technical and socio-technical factors,
- the definition of a model of an enterprise that is relevant to achieving safety and is applicable at different levels of abstraction,
- the definition of a safety engineering process applicable to socio-technical systems, and
- most importantly, the definition of principles to apply in the design, operation, maintenance and evolution of an enterprise to achieve and maintain its safety goals.

The above contributions provide a means for enterprises responsible to dangerous technologies to improve their safety management practices. The SEE approach better identifies factors that can lead to accidents and take them into account in the design, operations, maintenance and evolution of the enterprise and its technologies.

The SEE approach was compared to practices in the nuclear industry and shown to be better able to handle the complexities of a socio-technical system such as an enterprise. The nuclear industry was chosen because of its strict safety requirements and well documented safety practices.

13.2 Limitations

The approach was derived from and demonstrated within the nuclear industry. The process and models defined within the approach are not nuclear specific and so are applicable in other industry sectors. However, the principles defined within the approach are based on the nuclear industry and hence would require some mapping and translation to be useful in other industries.

13.3 Future Work

This thesis developed the SEE approach and demonstrated its effectiveness using a limited scope example in the nuclear industry. Future work includes:

- Extending the detail in the definition of the SEE approach to provide more detailed and complete guidance,
- Extending the scope of the example used to demonstrate the effectiveness of the approach, and
- Extending the approach to other industry sectors outside the nuclear industry.

Each of these scopes of future work could be taken independently but would benefit if they were done in an integrated manner with a specific target audience in mind.

For example, if another industry sector were chosen as the target audience of the future work then the future work would focus on meeting the needs of that sector. The improvement to the detail and guidance would take into account the specific needs of the targeted industry sector. The broader example used to demonstrate effectiveness would focus on aspects that are most relevant to that sector. The principles and terminology would be extended to take into account the terms and concepts commonly used in that sector.

13.3.1 Extending the SEE Approach

Since the scope of this thesis is very broad, some areas of the definition of the SEE approach did not drill down into great detail.

Each of the steps in the system engineering process were described generally in section 5.1. More specific guidance could be developed in the context of safety enterprise engineering to aid people in the application of the approach and the incorporation of the design principles necessary to deal with sources of unsafe control actions.

The application of STPA hazard analysis is sensitive to the safety control structure defined. Future work could develop more specific guidance for the development of safety control structures. This work could include more guidance on the relationships between the safety control structure design view and the other design views beyond that provided in section 7.3.5.

13.3.2 Extending the Example Application of the SEE Approach

Chapter 11 demonstrates the SEE approach using a very limited slice of safety related functionality of a typical nuclear utility. Table 22 shows the coverage of the weaknesses in nuclear practices by the scope of the example. Clearly a larger scope example could be undertaken that provides coverage of the weaknesses not covered by the example in this thesis.

13.3.3 Extending the SEE Approach to Other Industry Sectors

The work in this thesis focuses primarily on the nuclear industry. Future work could include reverse engineering principles from other industries as well as mapping the nuclear industry principles into the context of other industries. This will provide a more complete set of design principles and extend the applicability of the approach.

14 REFERENCES

[1] *Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants*. Washington, D.C.: National Academies Press, 2014.

[2] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press, 2012.

[3] P. Joannou, "Enterprise, Systems, and Software Engineering - The Need for Integration," *Computer*, 2007.

[4] S. Birla, "RESEARCH INFORMATION LETTER 1101: Technical basis to review hazard analysis of digital safety systems," p. 169.

[5] J. L. G. Dietz and J. A. P. Hoogervorst, "A critical investigation of TOGAF-based on the enterprise engineering theory and practice," *Adv. Enterp. Eng. V*, pp. 76–90, 2011.

[6] J. L. Dietz *et al.*, "The discipline of enterprise engineering," *Int. J. Organ. Des. Eng.*, vol. 3, no. 1, pp. 86–114, 2013.

[7] J. A. P. Hoogervorst, *Enterprise Governance and Enterprise Engineering*. Springer, 2009.

[8] V. Goepp and P.-A. Millet, "Editorial," *Int. J. Comput. Integr. Manuf.*, vol. 24, pp. 971–973, Nov. 2011.

[9] M. Op 't Land, E. Proper, M. Waage, J. Cloo, and C. Steghuis, "The Results of Enterprise Architecting," in *Enterprise Architecture*, Springer Berlin Heidelberg, 2009.

[10] A. Pyster *et al.*, "Guide to the Systems Engineering Body of Knowledge (SEBoK) version 1.3." Hoboken, NJ: The Trustees of the Stevens Institute of Technology, 2014.

[11] "ISO/IEC GUIDE 51:2014 , Safety aspects — Guidelines for their inclusion in standards." ISO, 2014.

[12] DoD, "MIL-STD-882E - DEPARTMENT OF DEFENSE STANDARD PRACTICE - SYSTEM SAFETY." 2012.

[13] N. Leveson, N. Dulac, K. Marais, and J. Carroll, "Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems," *Organ. Stud.*, vol. 30, no. 2–3, pp. 227–249, 2009.

[14] S. Gherardi and D. Nicolini, "To transfer is to transform: the circulation of safety knowledge," *Organization*, vol. 7, no. 2, pp. 329–348, 2000.

[15] N. Dulac and N. Leveson, "An approach to design for safety in complex systems," in *Int. Symposium on Systems Engineering (INCOSE)*, 2004.

[16] J. L. G. Dietz, "Enterprise ontology-understanding the essence of organizational operation," *Enterp. Inf. Syst. VII*, pp. 19–30, 2006.

[17] "Enterprise Modelling," *Prod. Plan. Control*, vol. 12, pp. 107–109, Jan. 2001.

[18] N. Letsinger and E. Ward, "Spotlight Article: Perspectives on Enterprise Modeling," *J. Enterp. Transform.*, vol. 1, pp. 179–184, Jul. 2011.

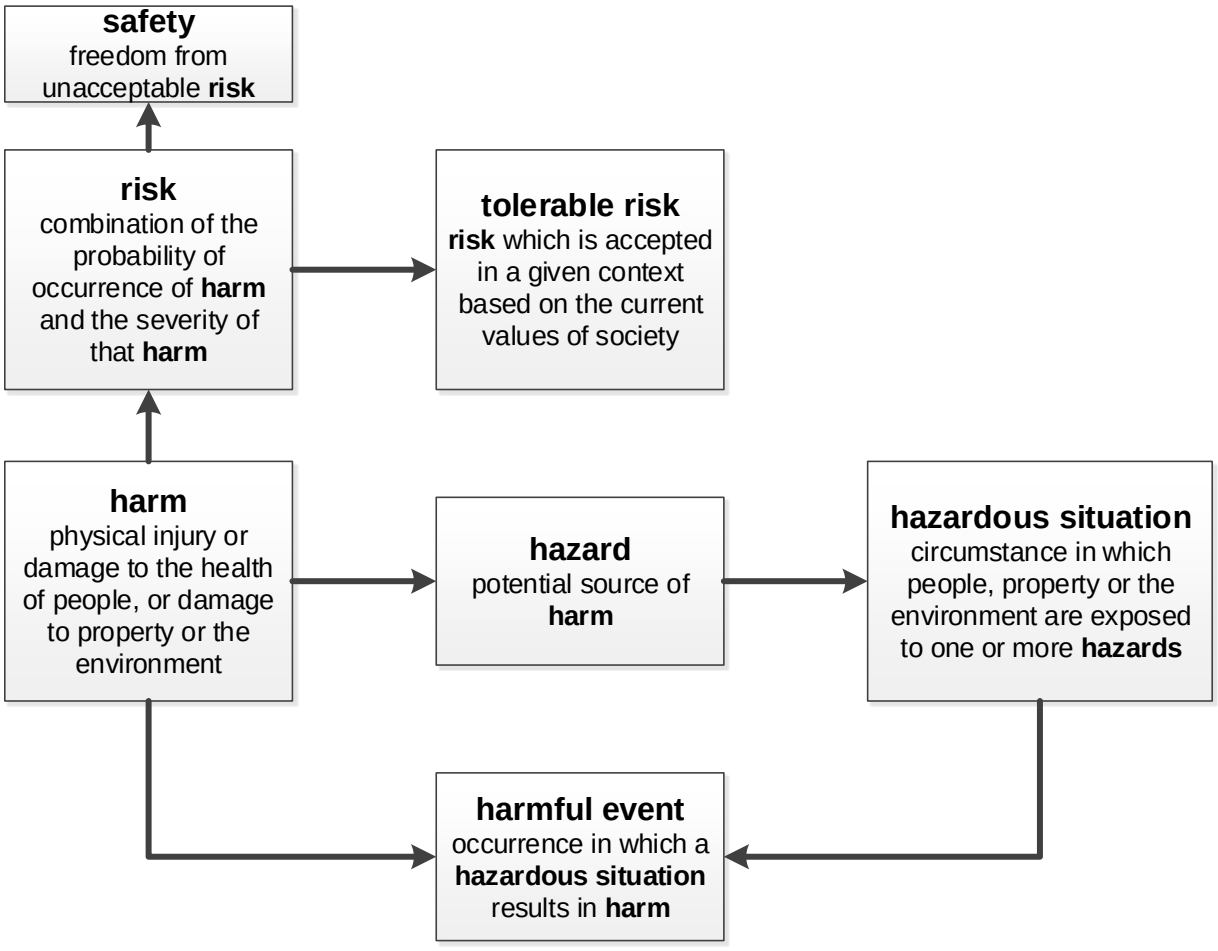
[19] IEC, "IEC 61508-4 - Functional safety of electrical/electronic/programmable electronic safety related systems - Part 4: Definitions and abbreviations." 2010.

[20] ISO and IEC, “ISO/IEC 15026-3 - Systems and software engineering - Systems and software assurance Part 3: System integrity levels.” 2015.
[21] ISO, “ISO 26262-1 - Road vehicles - Functional safety - Part 1:Vocabulary.” 2011.
[22] International Atomic Energy Agency, Ed., *IAEA safety glossary: terminology used in nuclear safety and radiation protection*, 2007 ed. Vienna, Austria: International Atomic Energy Agency, 2007.
[23] I. S. O. Guide, “ISO/IEC 15288 - Systems and software engineering — System life cycle processes,” *ISO Geneva Switz.*, 2009.
[24] ISO, “ISO 31000 - Risk management - Principles and guidelines.” 2009.
[25] ISO, “ISO 15704 - Industrial automation systems — Requirements for enterprise-reference architectures and methodologies.” 2000.
[26] ISO, “ISO 19439 - Enterprise integration — Framework for enterprise modelling.” 2006.
[27] ISO, “ISO 14258 - Industrial automation systems — Concepts and rules for enterprise models.” 1998.
[28] ISO, “ISO 19440 - Enterprise integration — Constructs for enterprise modelling.” ISO, 2007.
[29] ISO, IEC, and IEEE, “ISO/IEC/IEEE 42010 - Systems and software engineering — Architecture description.” 2011.
[30] W. E. Deming, *Out of the Crisis*. Massachusetts Inst Technology, 1982.
[31] International Atomic Energy Agency, *Safety of nuclear power plants: design.* Vienna: International Atomic Energy Agency, 2016.
[32] International Atomic Energy Agency, *Safety of nuclear power plants: commissioning and operation - no. ssr-2/2, rev. 1.* S.l.: Intl Atomic Energy Agency, 2016.
[33] “IEC 61226 Ed.3: Nuclear Power Plants – Instrumentation and control important to safety – Classification of instrumentation and control functions.” IEC, 2009.
[34] H. W. Heinrich, D. Petersen, and N. Roos, *Industrial Accident Prevention*. New York: McGraw-Hill, 1980.
[35] J. Reason, *Managing the Risks of Organizational Accidents*. Ashgate, 1997.
[36] N. G. Leveson, “STPA-An STPA Primer v1.” MIT Press, 2015.
[37] M. V. Stringfellow, “Accident analysis and hazard analysis for human and organizational factors,” Massachusetts Institute of Technology, 2010.
[38] Geary Rummler and A. Brache, *Improving performance : how to manage the white space on the organization chart*. 1995.
[39] W. J. Garland, “The Essential CANDU, A Textbook on the CANDU Nuclear Power Plant Technology.” University Network of Excellence in Nuclear Engineering (UNENE), 2014.
[40] “Equipment Reliability Process Description - AP-913 - Revision 2.” Institute for Nuclear Power Operation (INPO), 2007.
[41] “The Standard Nuclear Performance Model - A Process Management Approach.” Nuclear Energy Institute, 2003.
[42] *The operating organization for nuclear power plants: safety guide*. Vienna: International Atomic Energy Agency, 2001.

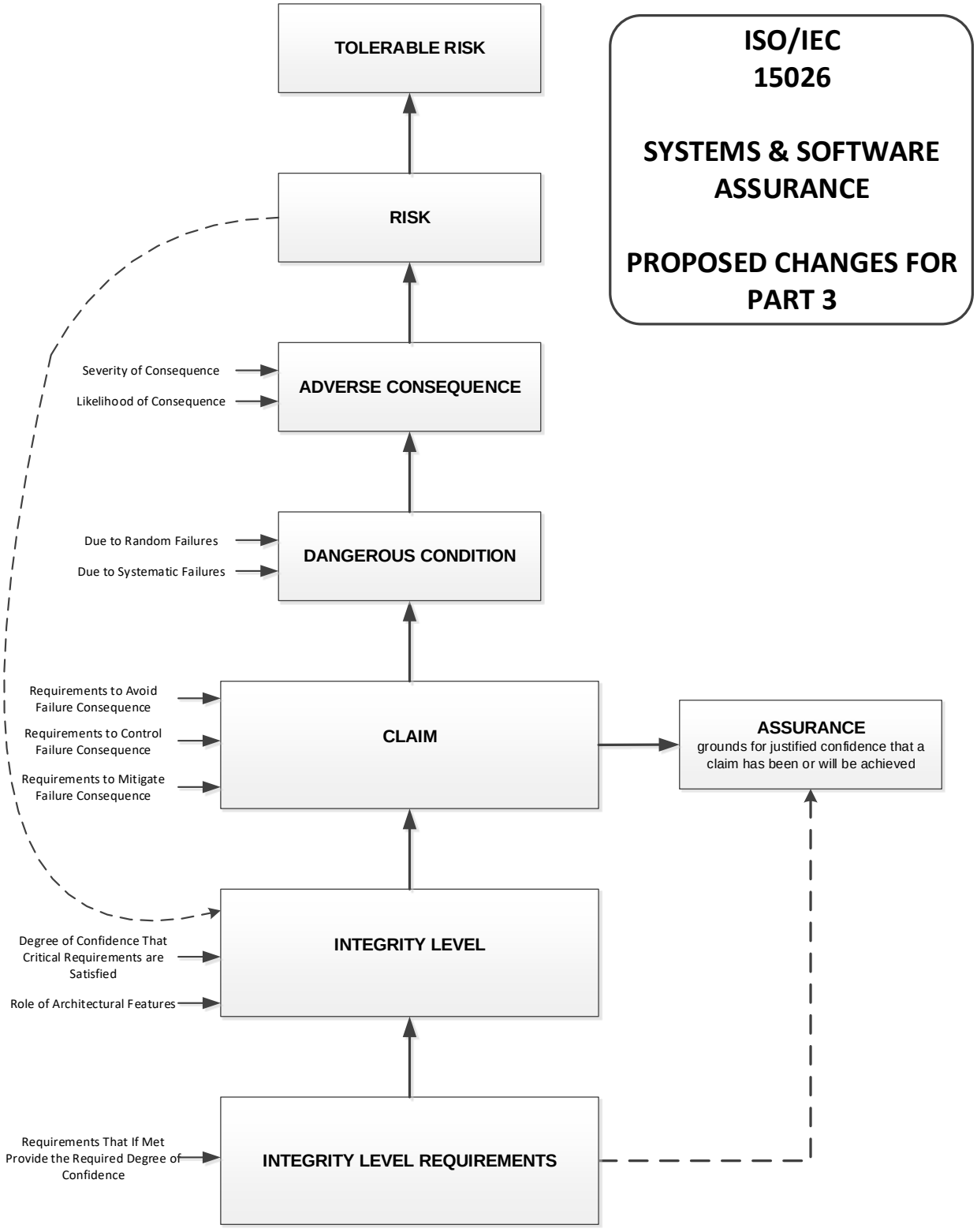
[43] International Atomic Energy Agency and Euratom, Eds., *Fundamental safety principles*. Vienna: International Atomic Energy Agency, 2006.
[44] International Nuclear Safety Advisory Group and International Atomic Energy Agency, Eds., *Basic safety principles for nuclear power plants: 75-INSAG-3 Rev. 1*, Rev. Vienna: International Atomic Energy Agency, 1999.
[45] *Defence in depth in nuclear safety: a report*. Vienna: International Atomic Energy Agency, 1996.
[46] INTERNATIONAL ATOMIC ENERGY AGENCY, *LEADERSHIP AND MANAGEMENT FOR SAFETY.* Place of publication not identified: INTL ATOMIC ENERGY AGENCY, 2016.
[47] Canadian Nuclear Safety Commission, CNSC Fukushima Task Force (Canada), and Depository Services Program (Canada), *CNSC Fukushima Task Force report*. Ottawa: Canadian Nuclear Safety Commission, 2011.
[48] "Fukushima Nuclear Accident Analysis Report." TEPCO, 2012.
[49] Nuclear Emergency Response Headquarters and Government of Japan, "Report of the Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations -." 2011.
[50] Japan Nuclear Technology Institute, "Examination of Accident at Tokyo Electric Power Co., Inc.'s Fukushima Daiichi Nuclear Power Station and Proposal of Countermeasures." Japan Nuclear Technology Institute, 2011.
[51] "Executive Summary of the Final Report - Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company." 2012.
[52] REPORT BY THE DIRECTOR GENERAL, "The Fukushima Daiichi Accident." IAEA, 2015.
[53] "Lessons Learned from the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station." INPO, 2012.
[54] International Atomic Energy Agency, *Governmental, legal and regulatory framework for safety: no. gsr part 1, rev. 1.* S.l.: Intl Atomic Energy Agency, 2016.
[55] International Atomic Energy Agency, *Establishing the safety infrastructure for a nuclear power programme.* Vienna: IAEA, 2011.
[56] "CNSC Regulatory Documents." CNSC, Aug-2017.
[57] "REGDOC-2-3-3 Operating Performance: Periodic Safety Reviews." CNSC, 2015.
[58] "Nuclear Safety Control Act." Government of Canada, 1997.
[59] "REGDOC-2-5-2 Physical Design: Design of Reactor Facilities Nuclear Power Plants." CNSC, 2014.
[60] International Atomic Energy Agency, *Periodic safety review for nuclear power plants: specific safety guide*. Vienna: International Atomic Energy Agency, 2013.

APPENDIX 1 – Key Terms in Source Documents for Definitions

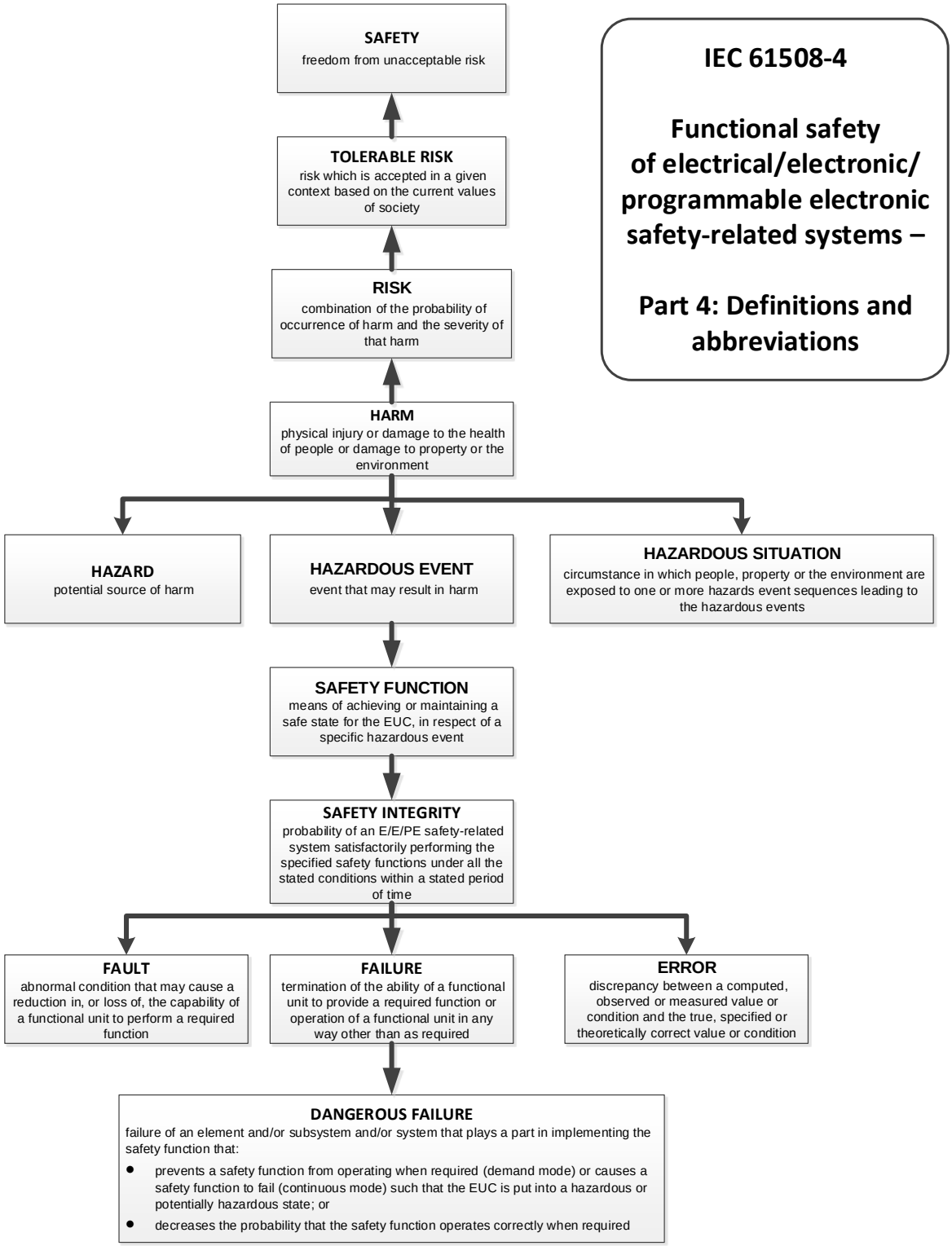
ISO/IEC Guide 51



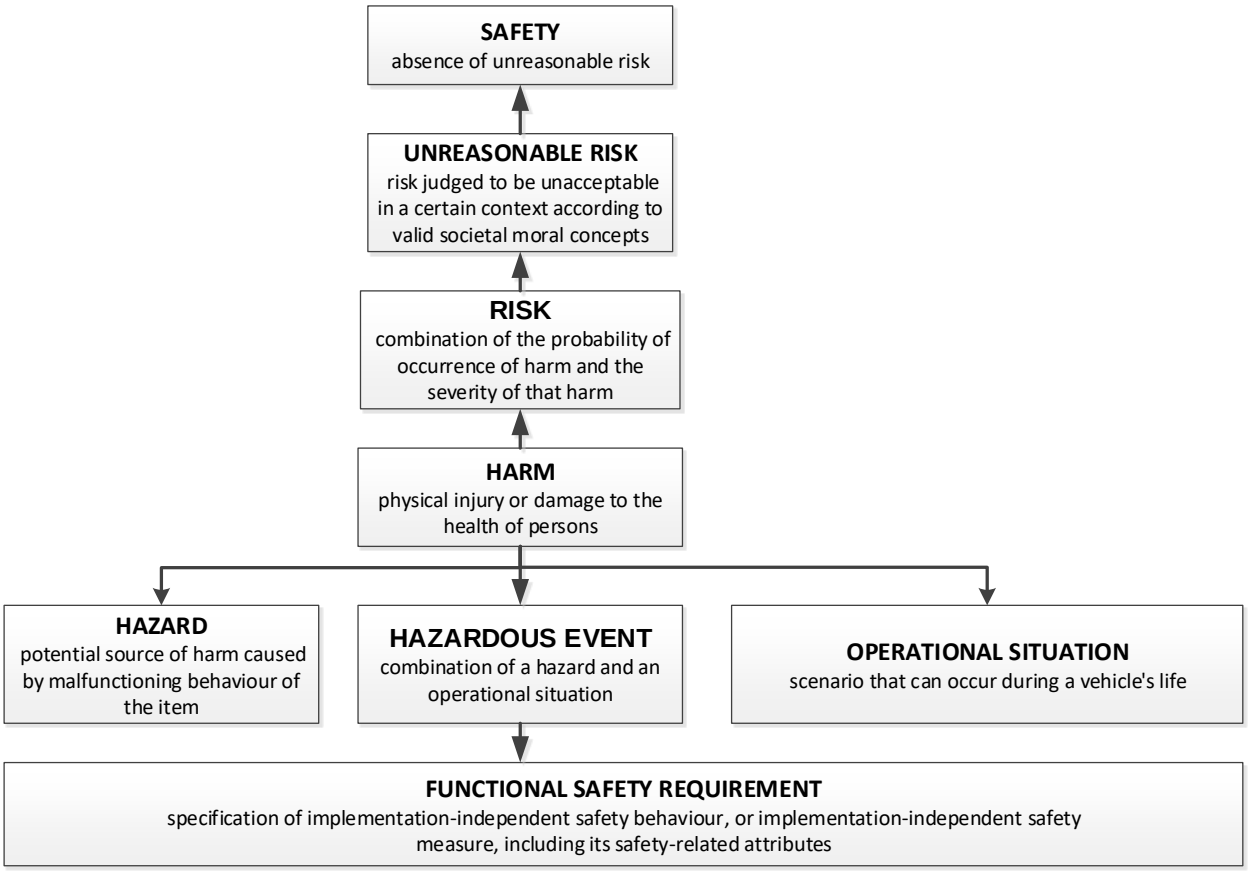
ISO/IEC 15026-3



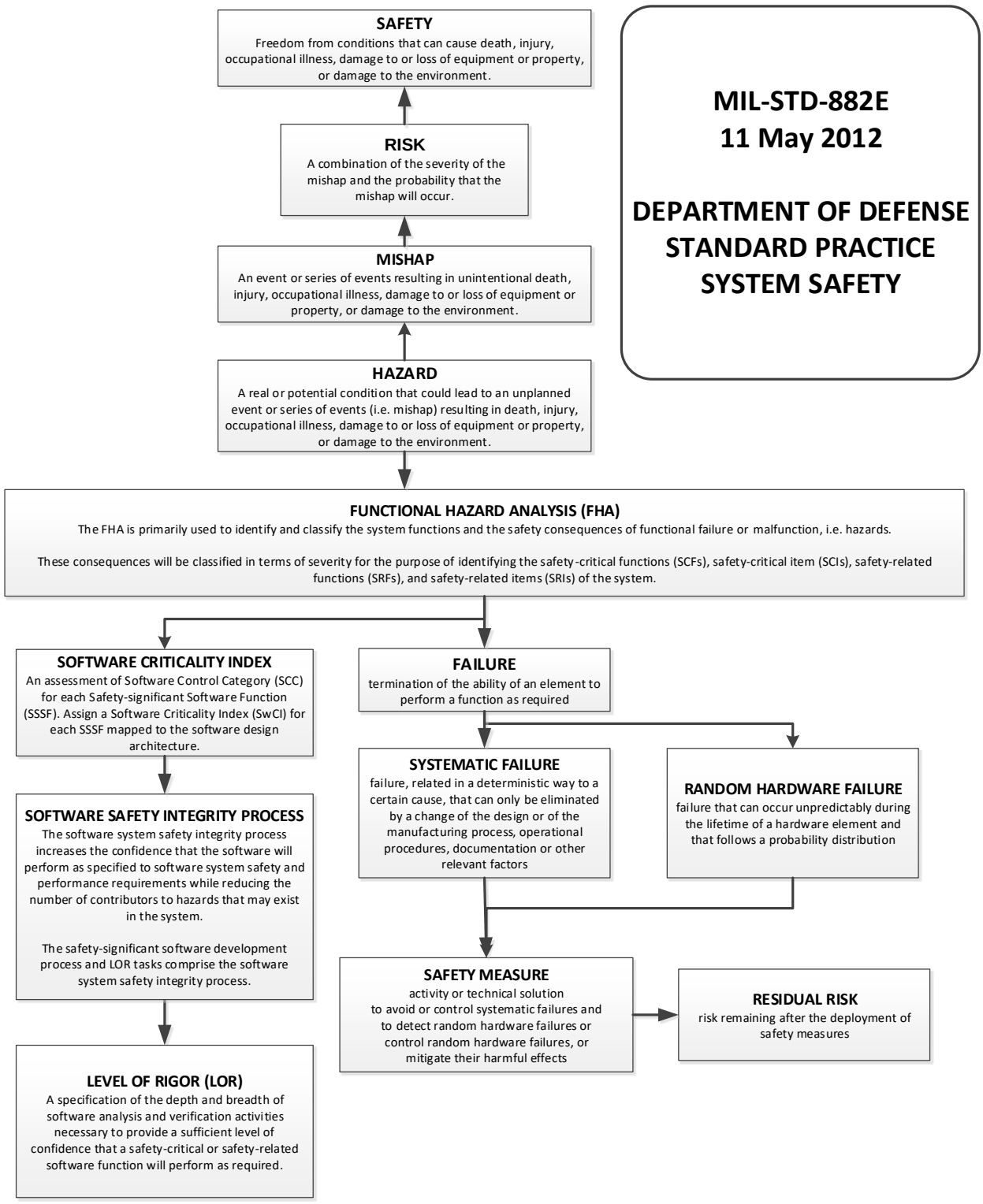
IEC 61508-4


SAFETY
freedom from unacceptable risk
TOLERABLE RISK
risk which is accepted in a given context based on the current values of society
RISK
combination of the probability of occurrence of harm and the severity of that harm
HARM
physical injury or damage to the health of people or damage to property or the environment
HAZARD
potential source of harm
HAZARDOUS EVENT
event that may result in harm
HAZARDOUS SITUATION
circumstance in which people, property or the environment are exposed to one or more hazards event sequences leading to the hazardous events
SAFETY FUNCTION
means of achieving or maintaining a safe state for the EUC, in respect of a specific hazardous event
SAFETY INTEGRITY
probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time
FAULT
abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function
FAILURE
termination of the ability of a functional unit to provide a required function or operation of a functional unit in any way other than as required
ERROR
discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition
DANGEROUS FAILURE
failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:
prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or
decreases the probability that the safety function operates correctly when required
IEC 61508-4
Functional safety of electrical/electronic/ programmable electronic safety-related systems –
Part 4: Definitions and abbreviations

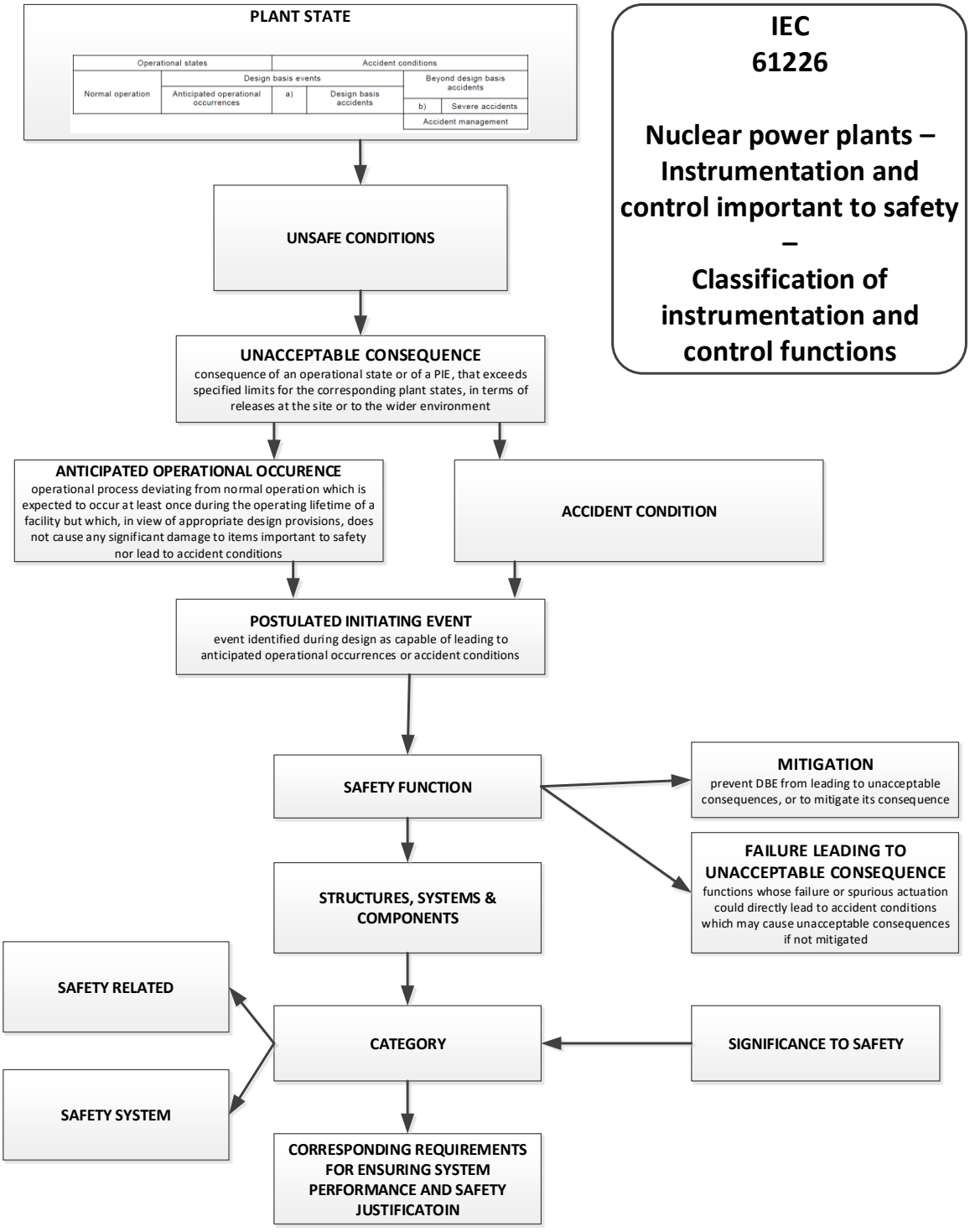
ISO 26262-1


SAFETY
absence of unreasonable risk
UNREASONABLE RISK
risk judged to be unacceptable in a certain context according to valid societal moral concepts
RISK
combination of the probability of occurrence of harm and the severity of that harm
HARM
physical injury or damage to the health of persons
HAZARD
potential source of harm caused by malfunctioning behaviour of the item
HAZARDOUS EVENT
combination of a hazard and an operational situation
OPERATIONAL SITUATION
scenario that can occur during a vehicle's life
FUNCTIONAL SAFETY REQUIREMENT
specification of implementation-independent safety behaviour, or implementation-independent safety measure, including its safety-related attributes

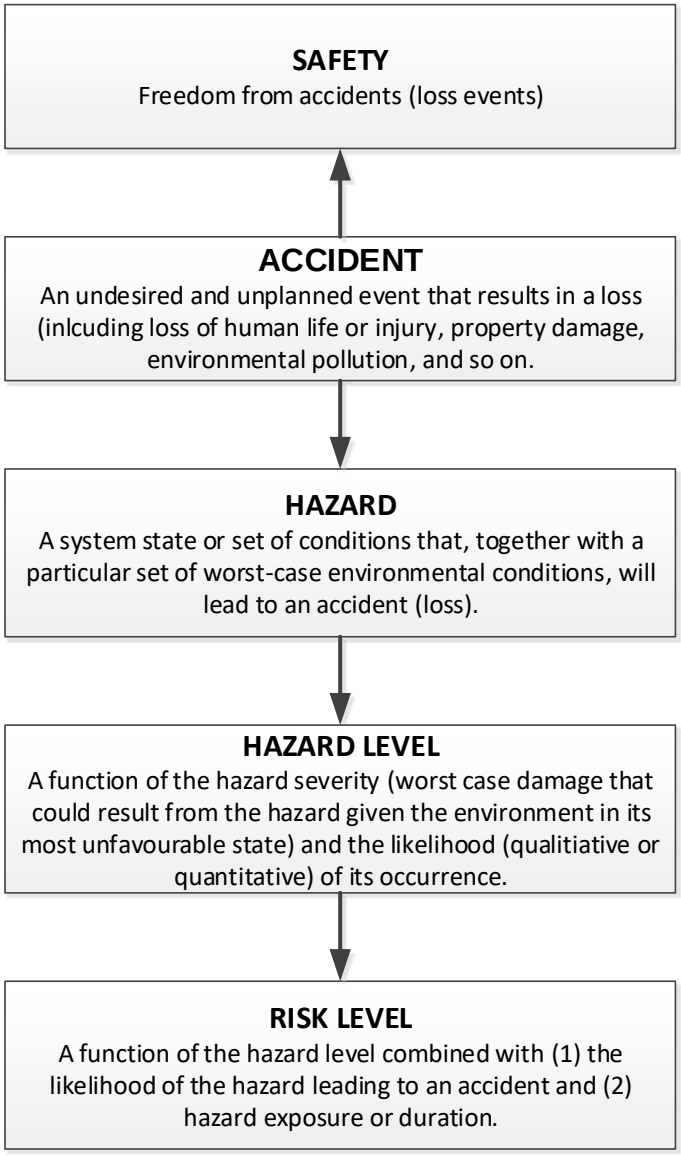
MIL-STD-882E


SAFETY
Freedom from conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
RISK
A combination of the severity of the mishap and the probability that the mishap will occur.
MISHAP
An event or series of events resulting in unintentional death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
HAZARD
A real or potential condition that could lead to an unplanned event or series of events (i.e. mishap) resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.
MIL-STD-882E
11 May 2012
DEPARTMENT OF DEFENSE
STANDARD PRACTICE
SYSTEM SAFETY
FUNCTIONAL HAZARD ANALYSIS (FHA)
The FHA is primarily used to identify and classify the system functions and the safety consequences of functional failure or malfunction, i.e. hazards.
These consequences will be classified in terms of severity for the purpose of identifying the safety-critical functions (SCFs), safety-critical item (SCIs), safety-related functions (SRFs), and safety-related items (SRIs) of the system.
SOFTWARE CRITICALITY INDEX
An assessment of Software Control Category (SCC) for each Safety-significant Software Function (SSSF). Assign a Software Criticality Index (SwCI) for each SSSF mapped to the software design architecture.
SOFTWARE SAFETY INTEGRITY PROCESS
The software system safety integrity process increases the confidence that the software will perform as specified to software system safety and performance requirements while reducing the number of contributors to hazards that may exist in the system.
The safety-significant software development process and LOR tasks comprise the software system safety integrity process.
LEVEL OF RIGOR (LOR)
A specification of the depth and breadth of software analysis and verification activities necessary to provide a sufficient level of confidence that a safety-critical or safety-related software function will perform as required.
FAILURE
termination of the ability of an element to perform a function as required
SYSTEMATIC FAILURE
failure, related in a deterministic way to a certain cause, that can only be eliminated by a change of the design or of the manufacturing process, operational procedures, documentation or other relevant factors
RANDOM HARDWARE FAILURE
failure that can occur unpredictably during the lifetime of a hardware element and that follows a probability distribution
SAFETY MEASURE
activity or technical solution to avoid or control systematic failures and to detect random hardware failures or control random hardware failures, or mitigate their harmful effects
RESIDUAL RISK
risk remaining after the deployment of safety measures

IAEA Safety Glossary / IEC 61226



Engineering a Safer World



APPENDIX 2 – Definitions of Enterprise Modeling Constructs

Organizational Unit

The Organizational Unit construct represents an entity of the organizational structure of an enterprise, which is described by attributes of the organization and references to both lower- and higher-level organizational entities. [28]

Organizational Units represent the formal, hierarchical or administrative structure of an enterprise, or some combination thereof. Its content is determined by naming the assigned entities for which it has responsibility. Position in the hierarchy are represented by the definition of the assignments of lower level units to the current unit and its own assignment to higher-level units. The construct enables multidimensional organization structures (i.e. matrix organizations, network organizations and others) by allowing multiple relationships to higher-level units.

Each Organizational Unit contains at least one relationship to an Organizational Role specifying the required organizational skills and responsibilities. Table 23 defines the attributes and relationships for an Organizational Unit.

Table 23 - Organizational Unit

ATTRIBUTES	
Name:	name of the Organizational Unit
Description:	textual description of the purpose of the Organizational Unit
RELATIONSHIPS	
Process Responsibilities:	identifying the Business Processes and Enterprise Activities for which this Organizational Unit has responsibility

People Responsibilities:	identifying the Person Profiles for which this Organizational Unit has responsibility
Assigned Organizational Units:	identifying the Organizational Units that are assigned to this Organizational Unit
Assigned Organizational Roles:	identifying the Organizational Roles that are assigned to this Organizational Unit
Assigned to Organization Units:	identifying the Organizational Units which have responsibility for this Organizational Unit
Assigned Decision Centres:	Identifying the Decision Centres that are assigned to this Organizational Unit

Organizational Role

Organizational Roles represent, within a given hierarchical structure of an enterprise, the organizationally relevant human skills and responsibilities required and provided to perform those organizational responsibilities that are assigned to the particular Organizational Role.

The enterprise's hierarchical structure is represented by Organizational Units and Decision Centres.

Each Organizational Role contains at least one relationship to an Organizational Unit. The relationships between Organizational Roles and Organizational Units are described by means of an assignment attribute in the design specification and later phases. Table 24 defines the attributes and relationships for an Organizational Role.

Table 24 - Organizational Role

ATTRIBUTES	
Name:	name of the Organizational Role
Responsibilities:	textual description of organizational, decision-making or problem solving responsibilities given to this Organizational Role
Organizational Skills:	skills which are required for organizational, decision-making and problem-solving responsibilities
RELATIONSHIPS	
Specialization of:	Organizational Roles that are a generalization of this particular instance
Responsible Organization Unit:	Organizational Unit that has responsibility for this Organizational Role
Assigned Decision Centre:	Decision Centre that is assigned to this Organizational Role

Person Profile

The Person Profile is a construct that represents a set of personal skills and responsibilities that are required by an Organizational Unit or an Enterprise Activity, or both, and that are provided by a person.

Person Profiles represent the human skills that are actually or potentially relevant for the work of Organizational Units and Enterprise Activities. A skill profile is a list of predefined or user-defined human organizational and operational skills, described in terms appropriate to the user of those skills and understandable to the person providing them.

Each Person Profile contains at least one relationship to an Organizational Unit. The relationships between Person Profiles and Organizational Units are described by means of an assignment attribute in the design specification and later phases. Table 25 defines the attributes and relationships for a Person Profile.

Table 25 - Person Profile

ATTRIBUTES	
Name:	name of the Person Profile
Organization-related Skills:	skills which are provided for organizational, decision-making and problem-solving tasks
Operation-related Skills:	skills which are provided for operational tasks
Role Job Description:	textual description of organizational, decision-making, problem-solving or operational tasks
RELATIONSHIPS	
Assigned to Organizational Units:	Organizational Unit that has responsibility for this Person Profile

Assigned to Organizational Role:	Organizational Roles to which this Person Profile is assigned

Capability

A Capability is a construct that represents the collection of capability characteristics (expressed as capability attributes) of either a Resource (its provided Capability) or an Enterprise Activity (its required Capability).

A Capability describes, by means of capability attributes and other included Capabilities, the functionality which is needed and provided to support the execution of the task to be performed by an Enterprise Activity, and identifies constraints determined by the things to be processed (such as safety and security aspects, certain tooling and working space dimensions, data processing/storing and main memory/storage capacity, etc.) and possibly time restrictions.

Capability attributes are defined in terms of a Resource-dependant attribute and a value, set of values, or permissible range of values for that attribute. Table 26 defines the attributes and relationships for a Capability.

Table 26 - Capability

ATTRIBUTES	
Name:	name of this Capability
Description:	textual description of the Capability
Performance-related Attributes:	identifying and constraining performance-related attributes of one or more Resource instances
Operation-related Attributes:	identifying and constraining Enterprise Activity-related attributes of one or more Resource instances

RELATIONSHIPS	
Capabilities Included:	names of included Capability instances
Where required:	Enterprise Activities that require an instance of this Capability
Where provided:	Resources that provide instances of this Capability
Operation Responsibility:	Organizational Role and Organizational Unit respectively responsible for this instance

Resource

A Resource is a construct that is a specialization of the Enterprise Object construct, which represents the provided capabilities available to execute an Enterprise Activity.

A Resource represents some or all of the capabilities provided for an Enterprise Activity according to its required capabilities, where these capabilities are those of any device, tool or means30) at the disposal of the enterprise to produce goods or services. A Resource is a specialization of Enterprise Object that specializes the attribute properties and adds new attributes:

– provided operational roles, and

– provided capability.

The resulting construct template has a distinguishing construct label to reflect its purpose and usage.

For each kind of Resource, all relevant qualities and services of that Resource are described in terms of a Capability (see 6.11), related to its ability to complete functional operations in the enterprise and its availability for, and constraints on, carrying out those tasks. The corresponding functions for acquiring or preserving the ability and the availability respectively (i.e. preparation, provision, servicing),

as well as the logical sequence of these functions, should also be described. Table 27 defines the attributes and relationships for a Resource.

Table 27 - Resource

ATTRIBUTES	
Name:	name of the Resource
Description:	textual description of the purpose of the Organ
Properties:	elements representing properties and their values of the Resource instance
RELATIONSHIPS	
Provided Operational Roles:	Operational Roles providing human capabilities to operate this Resource instance
Provided Capability:	provided Capabilities of this Resource instance
Specialization of:	Resource classes which are a generalization of this particular instance
Related to:	Enterprise Object instances that are related to this Resource instance
Operation Responsibility:	Organizational Role and Organizational Unit respectively, having responsibility for operation of this instance

Enterprise Object

An Enterprise Object is a construct that represents a piece of information in the enterprise and that describes a generalized or a real or an abstract entity which can be conceptualized as being a whole.

An Enterprise Object represents the common characteristics from an information viewpoint of a thing (an enterprise entity) as it exists during its lifetime. Its usage is restricted to those situations where only the information aspects of the entity under consideration are relevant. Table 27 defines the attributes and relationships for an Enterprise Object.

Table 28 - Enterprise Object

ATTRIBUTES	
Name:	name of the Enterprise Object
Description:	textual description of the Enterprise Object
Properties:	elements representing properties and their values of the Enterprise Object instance
RELATIONSHIPS	
Specialization of:	Enterprise Objects which are a generalization of this particular instance
Related to:	Enterprise Object instances that are related to this Enterprise Object instance
Operation Responsibility:	Organizational Role and Organizational Unit respectively, having responsibility for operation of this instance

Decision Centre

A Decision Centre is a construct that represents a set of decision-making activities that are characterized by having the same time horizon and planning period and belonging to the same kind of functional category.

Decision Centres represent the decisional structure of an enterprise. A decisional structure is defined when the set of decision centres are known and their relations determined.

The Decision Centre construct describes identifiable entities together with their position relative to other such entities in the enterprise decision structure. The Decision Centre content are determined by a set of decisions (and decision-making activities) belonging to the Centre and by decision frame attributes (objectives, variables, constraints, etc.). Table 29 defines the attributes and relationships for a Decision Centre.

Table 29 - Decision Centre

ATTRIBUTES	
Name:	name of the Decision Centre
Description:	textual description of the Decision Centre
Objectives:	objectives to be achieved
Organization Level:	textual description of the level of this Decision Centre in relation to the organization hierarchy
RELATIONSHIPS	
Process applicability:	which Business Processes and Enterprise Activities decisions made by this Decision Centre apply

Assigned Decision Centres:	Decision Centres controlled by this Decision Centre
Assigned to Decision Centre:	Decision Centre that has responsibility for this Decision Centre
Assigned to Organization Role:	Organizational Role responsible for the Decision Centre
Assigned to Organization Unit:	Organizational Unit to which this Decision Centre is assigned

Business Process

A Business Process is a construct that represents a partially ordered set of Business Processes or Enterprise Activities, or both, that can be executed to realize one or more given objectives of an enterprise or a part of an enterprise to achieve some desired end-result.

A Business Process construct describes the functionalities needed to produce a desired result that satisfies one or more business objectives derived from business objectives defined for the enterprise domain. This result emerges from transformations or combinations, or both, of entities into new entities or into new states which require appropriate control and functional capacity.

The internal structure of a Business Process is described in terms of a set of functionalities, decomposed according to modelling criteria (reduction of complexity) and the needs of operational monitoring and control. These internal functionalities are characterized as combinations of constituent Business Processes or Enterprise Activities, or both, and their interconnections, arranged by ordering relationships and dependencies described by behavioural rules, which capture the process dynamics.

The result of a Business Process is observable or quantifiable. It can result in material entities (such as industrial products), or information entities (such as orders, documents or data), or newly designed processes, or can be defined as the achievement of one or more designated objectives. Table 30 defines the attributes and relationships for a Business Process.

Table 30 - Business Process

ATTRIBUTES	
Name:	name of the Business Process
Description:	textual description of the Business Process
Objectives:	strategic and operational business objectives to be fulfilled by the Business Process instance
Performance Indicators:	measure by which achievement of the objectives can be assessed
RELATIONSHIPS	
Consists of:	Business Process and Enterprise Activity instances of which this Business Process instance is the aggregate
Input Enterprise Objects:	Enterprise Objects, instances of which are available for occurrences of the Business Process instance
Output Enterprise Objects:	Enterprise Objects, instances of which are made available by occurrences of the Business Process instance
Operation Responsibility:	Organizational Role and Organizational Unit respectively, having responsibility for operation of this instance

Enterprise Activity

An Enterprise Activity is a construct that represents a certain part of the lowest level of enterprise functionality required by user objectives and identifies the inputs needed for its execution and the outputs created as a result.

An Enterprise Activity construct identifies all things required for and produced by the execution of a particular task, which transforms function input(s) into function output(s) using control, operational role and resource inputs and optionally producing control, operational role and resource-related information outputs.

The latter contains status information on the execution of the task as they relate to the activity itself and the resource, respectively. Operational Role inputs identify required skills to be provided by assigned Person Profiles. Resource inputs shall identify the required and provided capabilities, respectively. Table 31 defines the attributes and relationships for an Enterprise Activity.

Table 31 - Enterprise Activity

ATTRIBUTES	
Name:	name of the Enterprise Activity
Description:	textual description of the Enterprise Activity
Objectives:	strategic and operational business objectives to be fulfilled by the Enterprise Activity instance
Performance Indicators:	measure by which achievement of the objectives can be assessed
RELATIONSHIPS	
Consists of:	Enterprise Activity instances of which this Enterprise Activity instance is the aggregate

Where Used:	Business Process employing this Enterprise Activity
Function Inputs:	Enterprise Object instances describing input information to be processed by this Enterprise Activity instance
Control Inputs:	Enterprise Object instances describing input information providing run-time data used but not modified by occurrences of this Enterprise Activity instance
Required Operational Roles:	Operational Roles defining required operational capabilities of occurrences of this Enterprise Activity instance
Required Capabilities:	required capabilities of occurrences of this Enterprise Activity instance
Function Outputs:	Enterprise Object instances describing the information outputs produced by occurrences of this Enterprise Activity instance

Technology Element

A Technology Element is a construct that represents all or a component of a technological system that can potentially take on a hazardous state relative to a defined set of accidents. Table 32 defines the attributes and relationships for a Technology Element.

Table 32 - Technology Element

ATTRIBUTES	
Name:	name of the Technology Element

Description:	textual description of the Technology Element
Interfaces:	description of each interface between this element and another technology element

RELATIONSHIPS	
Consists of:	Technology Element instances of which this Technology Element instance is the aggregate
Where Used:	Technology Element interfacing to this Technology Element

APPENDIX 3 – Nuclear Best Practice Principles

This appendix lists requirements from the IAEA documents identified in section 8.1. The requirements are grouped by design phase that they impact (design and construction, operations and maintenance or performance monitoring and continuous improvement) and then whether they primarily impact business processes, organization, governance or the technology. For each requirement, the cause of the hazard addressed by the requirement and design features used to deal with the causes have been reverse engineered.

The ”Ref” column refers to the following source documents for the requirements:

1 International Atomic Energy Agency. 2016. Safety of Nuclear Power Plants: Design.

2 International Atomic Energy Agency. 2016. Safety of Nuclear Power Plants: Commissioning and Operation

3 International Atomic Energy Agency. 2016. Leadership and Management for Safety

4 International Atomic Energy Agency. 2016. Governmental, Legal and Regulatory Framework for Safety

5 International Atomic Energy Agency, and Euratom, eds. 2006. Fundamental Safety Principles.

6 International Nuclear Safety Advisory Group, and International Atomic Energy Agency, eds. 1999. Basic Safety Principles for Nuclear Power Plants

7 Defence in Depth in Nuclear Safety: A Report. 1996. INSAG 10. International Atomic Energy Agency.

DESIGN AND CONSTRUCTION PHASE

Business Process

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
18	1	Requirement 10: Safety assessment	Comprehensive deterministic safety assessments and probabilistic safety assessments shall be carried out throughout the design process for a nuclear power plant to ensure that all safety requirements on the design of the plant are met throughout all stages of the lifetime of the plant, and to confirm that the design, as delivered, meets requirements for manufacture and for construction, and as built, as operated and as modified.	4.17. The safety assessments shall be commenced at an early point in the design process, with iterations between design activities and confirmatory analytical activities, and shall increase in scope and level of detail as the design programme progresses. 4.18. The safety assessments shall be documented in a form that facilitates independent evaluation.	too low a likelihood that errors in the design that impact satisfaction of safety requirements are detected Operator performance inconsistent with performance assumed by the design Design change introduced new hazard that was not detected and confirmed to be addressed adequately by design	use of proven processes and methods for the engineering of the system as defined in appropriate codes and standards controlling changes to the design to ensure assurance that safety requirements are satisfied is maintained at the same level or better when changes are made to the design independent personnel perform V&V activities clear documentation of safe operating envelope and its incorporation into operating procedures
19	1	Requirement 11: Provision for construction	Items important to safety for a nuclear power plant shall be designed so that they can be manufactured, constructed, assembled, installed and erected in accordance with established processes that ensure the achievement of the design specifications and the required level of safety.	4.19. In the provision for construction and operation, due account shall be taken of relevant experience that has been gained in the construction of other similar plants and their associated structures, systems and components. Where best practices from other relevant industries are adopted, such practices shall be shown to be appropriate to the specific nuclear application.	Manufacturing error caused item to not satisfy safety requirements Construction error caused item to not satisfy safety requirement Installation error caused item to not satisfy safety requirement	The design of items important to safety shall take into account the attributes of manufacturability, constructability and installabilty to ensure that the probability of introduction of undetected errors is commensurate with the level of risk of errors. Operating experience from the design, construction and operation of similar plants shall be taken into account.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
20	1	Requirement 2: Management system for plant design	The design organization shall establish and implement a management system for ensuring that all safety requirements established for the design of the plant are considered and implemented in all phases of the design process and that they are met in the final design.	3.2. The management system shall include provision for ensuring the quality of the design of each structure, system and component, as well as of the overall design of the nuclear power plant, at all times. This includes the means for identifying and correcting design deficiencies, for checking the adequacy of the design and for controlling design changes 3.3. The design of the plant, including subsequent changes, modifications or safety improvements, shall be in accordance with established procedures that call on appropriate engineering codes and standards and shall incorporate relevant requirements and design bases. Interfaces shall be identified and controlled. 3.4. The adequacy of the plant design, including design tools and design inputs and outputs, shall be verified and validated by individuals or groups separate from those who originally performed the design work. Verification, validation and approval of the plant design shall be completed as soon as is practicable in the design and construction processes, and in any case before operation of the plant is commenced.	too high a likelihood that errors are introduced into the design that impact satisfaction of safety requirements too low a likelihood that errors in the design that impact satisfaction of safety requirements are detected	use of proven processes and methods for the engineering of the system as defined in appropriate codes and standards controlling changes to the design to ensure assurance that safety requirements are satisfied is maintained at the same level or better when changes are made to the design independent personnel perform V&V activities
22	1	Requirement 30: Qualification of items important to safety	A qualification programme for items important to safety shall be implemented to verify that items important to safety at a nuclear power plant are capable of performing their intended functions when necessary, and in the prevailing environmental conditions, throughout their design life, with due account taken of plant conditions during maintenance and testing.	5.48. The environmental conditions considered in the qualification programme for items important to safety at a nuclear power plant shall include the variations in ambient environmental conditions that are anticipated in the design basis for the plant. 5.49. The qualification programme for items important to safety shall include the consideration of ageing effects caused by environmental factors (such as conditions of vibration, irradiation, humidity or temperature) over the expected service life of the items important to safety. When the items important to safety are subject to natural external events and are required to perform a safety function during or following such an event, the qualification programme shall replicate as far as is practicable the conditions imposed on the items important to safety by the natural external event, either by test or analysis, or by a combination of both. 5.50. Any environmental conditions that could reasonably be anticipated and that could arise in specific operational states, such as in periodic testing of the containment leak rate, shall be included in the qualification programme.	Safety requirements do not fully take into account the variations in environmental conditions within which the system may have to safely operate. The qualification programme for items important to safety does not fully take into account all variations in environmental conditions within which the system may have to safely operate.	Use of effective hazard analysis techniques Use of competent personnel to perform hazard analysis Qualification programme complies with appropriate industry standards Qualification is performed by competent personnel

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
23	1	Requirement 31: Ageing management	The design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation, to ensure the capability of items important to safety to perform their necessary safety functions throughout their design life.	5.51. The design for a nuclear power plant shall take due account of ageing and wear out effects in all operational states for which a component is credited, including testing, maintenance, maintenance outages, plant states during a postulated initiating event and plant states following a postulated initiating event. 5.52. Provision shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help to identify unanticipated behaviour of the plant or degradation that might occur in service.	Effects of ageing not taken into account when establishing design margins	The design and verification processes take into account ageing and wearout mechanisms Competent personnel perform design and verification activities An effective ageing management is in place that monitors for ageing mechanisms and unanticipated behaviour of systems

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
24	1	Requirement 32: Design for optimal operator performance	Systematic consideration of human factors, including the human–machine interface, shall be included at an early stage in the design process for a nuclear power plant and shall be continued throughout the entire design process.	5.53. The design for a nuclear power plant shall specify the minimum number of operating personnel required to perform all the simultaneous operations necessary to bring the plant into a safe state. 5.54. Operating personnel who have gained operating experience in similar plants shall, as far as is practicable, be actively involved in the design process conducted by the design organization, in order to ensure that consideration is given as early as possible in the process to the future operation and maintenance of equipment. 5.55. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the likelihood and the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states. 5.56. The human–machine interface shall be designed to provide the operators with comprehensive but easily manageable information, in accordance with the necessary decision times and action times. The information necessary for the operator to make decisions to act shall be simply and unambiguously presented. 5.57. The operator shall be provided with the necessary information: (a) To assess the general state of the plant in any condition; (b) To operate the plant within the specified limits on parameters associated with plant systems and equipment (operational limits and conditions); (c) To confirm that safety actions for the actuation of safety systems are automatically initiated when needed and that the relevant systems perform as intended; (d) To determine both the need for and the time for manual initiation of the specified safety actions. 5.58. The design shall be such as to promote the success of operator actions with due regard for the time available for action, the conditions to be expected and the psychological demands being made on the operator. 5.59. The need for intervention by the operator on a short time scale shall be kept to a minimum, and it shall be demonstrated that the operator has sufficient time to make a decision and sufficient time to act. 5.60. The design shall be such as to ensure that, following an event affecting the plant, environmental conditions in the control room or the supplementary control room and in locations on the access route to the supplementary control room do not compromise the protection and safety of the operating personnel. 5.61. The design of workplaces and the working environment of the operating personnel shall be in accordance with ergonomic concepts. 5.62. Verification and validation, including by the use of simulators, of features relating to human factors shall be included at appropriate stages to confirm that necessary actions by the operator have been identified and can be correctly performed.	Operator performance inconsistent with performance assumed by the design	Assumptions on operations and maintenance performance necessary to achieve safety is clearly documented Design of operations and maintenance organizations are consistent with design assumptions on operations and maintenance performance Operations and maintenance personnel are involved in effective design reviews to ensure that assumptions on operations and maintenance performance are achieveable HMI supports achievement of operations and maintenance performance assumed in the design

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
25	1	Requirement 42: Safety analysis of the plant design	A safety analysis of the design for the nuclear power plant shall be conducted in which methods of both deterministic analysis and probabilistic analysis shall be applied to enable the challenges to safety in the various categories of plant states to be evaluated and assessed.	5.71. On the basis of a safety analysis, the design basis for items important to safety and their links to initiating events and event sequences shall be confirmed.18 It shall be demonstrated that the nuclear power plant as designed is capable of complying with authorized limits on discharges with regard to radioactive releases and with the dose limits in all operational states, and is capable of meeting acceptable limits for accident conditions. 5.72. The safety analysis shall provide assurance that defence in depth has been implemented in the design of the plant. 5.73. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases. 5.74. The applicability of the analytical assumptions, methods and degree of conservatism used in the design of the plant shall be updated and verified for the current or as built design.	Lack of comprehensive and correct traceability from safety requirements down into the design details Inadequate consideration for uncertainties in the design when establishing and verifying design margins	A safety analysis shall be performed and documented providing traceable evidence that the system will satisfy its safety requirements The safety analysis shall document the assumptions upon which it is based and the uncertainties upon which the design margins are based.
26	1	Requirement 9: Proven engineering practices	Items important to safety for a nuclear power plant shall be designed in accordance with the relevant national and international codes and standards.	4.14. Items important to safety for a nuclear power plant shall preferably be of a design that has previously been proven in equivalent applications, and if not, shall be items of high quality and of a technology that has been qualified and tested. 4.15. National and international codes and standards that are used as design rules for items important to safety shall be identified and evaluated to determine their applicability, adequacy and sufficiency, and shall be supplemented or modified as necessary to ensure that the quality of the design is commensurate with the associated safety function. 4.16. Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected.	use of items that do not have adequate supporting evidence that they are fit for purpose Lacking adequate: - operating history - use of applicable codes and standards in its engineering - test results - research results - in service monitoring of its performance	qualification process compliant with applicable codes and standards

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
43	2	Requirement 25: Commissioning programme	The operating organization shall ensure that a commissioning programme for the plant is established and implemented.	6.1. The commissioning programme for the plant shall cover the full range of plant conditions required in the design and the safety case. The results shall be used to demonstrate that the behaviour of the plant as built is in compliance with the design assumptions and the licence conditions. Special attention shall be paid to ensuring that no commissioning tests are performed that might place the plant in an unanalysed condition. Commissioning stages, test objectives and acceptance criteria shall be specified in such a way that the programme is auditable. 6.2. The commissioning programme shall provide the operating organization and the regulatory body with the means of identifying the hold points in the commissioning process at which approval may be required prior to continuing to the next stage. 6.3. The commissioning programme shall be divided into stages. A review of the test results for each stage shall be completed before commissioning is continued to the next stage. On the basis of the review, a judgement shall be made on whether the commissioning programme can proceed to the next stage. Judgements shall also be made on the basis of the review on whether the succeeding stages will be modified as a consequence of the test results, or because some tests in the stage had not been undertaken, or some tests had been undertaken but had not been completed. The results for some stages may be subject to approval by the regulatory body before commissioning can proceed to the next stage. 6.4. The commissioning programme shall include all the tests necessary to demonstrate that the plant as built and as installed meets the requirements of the safety analysis report and satisfies the design intent and, consequently, that the plant can be safely operated in accordance with the operational limits and conditions. 6.5. Operating and maintenance procedures shall be validated to the extent practicable as part of the commissioning programme, with the participation of future operating personnel. 6.6. Suitably qualified operations personnel shall be directly involved in the commissioning process. Operating personnel and plant technical staff shall be involved in the commissioning process to the extent necessary to ensure proper preparation for the operational phase. 6.7. The commissioning programme shall be sufficiently comprehensive as to provide reference data to characterize structures, systems and components. Such reference data shall be retained as they are important for ensuring the safety of the plant and for subsequent safety reviews. 6.8. All the functions of the operating organization shall be performed at the appropriate stages during commissioning. These functions shall include discharging responsibilities for management, training of personnel, the radiation protection programme, waste management, managements of records, fire safety, physical protection and the emergency plan. 6.9. Operating procedures and test procedures shall be verified to ensure their technical accuracy and shall be validated to ensure their usability with the installed equipment and control systems. Verification and validation of procedures shall be performed to confirm their applicability and quality, and to the extent possible shall be performed prior to fuel handling operations on the site. This process shall continue during the commissioning phase. Verification and validation shall also be carried out for procedures for overall operation. 6.10. From the commencement of commissioning, reviewed and approved arrangements for work control, modification control and plant configuration control shall be in place to meet the conditions of the commissioning tests. 6.11. Initial fuel loading shall not be authorized until all relevant pre-operational tests have been performed and the results have been accepted by the operating organization and the regulatory body. Reactor criticality and initial power increase shall not be authorized until all necessary tests have been performed and the results have been accepted by the operating organization and the regulatory body, as appropriate. The tests of the commissioning programme shall be successfully completed as a necessary condition for authorization, as appropriate, for normal operation of the plant to be commenced.	System, as designed, manufactured, constructed and installed does not satisfy safety requirements AND commissioning program was not adequate to detect the deficiency	Comprehensive commissioning program addressing all safety related requirements Comprehensive commissioning program addressing all safety related operating procedures Competent personnel planning and executing the commissioning program

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
47	3	Requirement 10: Management of processes and activities	Processes and activities shall be developed and shall be effectively managed to achieve the organization's goals without compromising safety.	4.28. Each process shall be developed and shall be managed to ensure that requirements are met without compromising safety. Processes shall be documented and the necessary supporting documentation shall be maintained. It shall be ensured that process documentation is consistent with any existing documents of the organization. Records to demonstrate that the results of the respective process have been achieved shall be specified in the process documentation. 4.29. The sequencing of a process and the interactions between processes shall be specified so that safety is not compromised. Effective interaction between interfacing processes shall be ensured. Particular consideration shall be given to interactions between processes within the organization, and to interactions between processes conducted by the organization and processes conducted by external service providers. 4.30. New processes or modifications to existing processes shall be designed, verified, approved and applied so that safety is not compromised. Processes, including any subsequent modifications to them, shall be aligned with the goals, strategies, plans and objectives of the organization. 4.31. Any activities for inspection, testing, and verification and validation, their acceptance criteria and the responsibilities for carrying out such activities shall be specified. It shall be specified when and at what stages independent inspection, testing, and verification and validation are required to be conducted. 4.32. Each process or activity that could have implications for safety shall be carried out under controlled conditions, by means of following readily understood, approved and current procedures, instructions and drawings. These procedures, instructions and drawings shall be validated before their first use and shall be periodically reviewed to ensure their adequacy and effectiveness. Individuals carrying out such activities shall be involved in the validation and the periodic review of such procedures, instructions and drawings.	Incorrect execution of the engineering process resulting in non-compliance with safety requirements as a consequence of: - lack of clear communications on the expectations of the engineering process - lack of management controls on the execution of the engineering process - lack of effective verification of the engineering process	Clear documentation of the engineering process Comprehensive training of personnel in the expectations of the engineering process Effective management oversight of the engineering process
27	3	Requirement 11: Management of the supply chain	The organization shall put in place arrangements with vendors, contractors and suppliers for specifying, monitoring and managing the supply to it of items, products and services that may influence safety.	4.33. The organization shall retain responsibility for safety when contracting out any processes and when receiving any item, product or service in the supply chain 4.34. The organization shall have a clear understanding and knowledge of the product or service being supplied. The organization shall itself retain the competence to specify the scope and standard of a required product or service, and subsequently to assess whether the product or service supplied meets the applicable safety requirements. 4.35. The management system shall include arrangements for qualification, selection, evaluation, procurement, and oversight of the supply chain. 4.36. The organization shall make arrangements for ensuring that suppliers of items, products and services important to safety adhere to safety requirements and meet the organization's expectations of safe conduct in their delivery.	Safety requirements for procured items and services were not completely and correctly specified Inadequate qualification of procured items and services to confirm that they comply with safety requirements Behaviour of procured items creates hazards that were not taken into account in the design	Technical specifications for items important to safety shall be developed using appropriate methods that result in complete and correct specifications of safety requirements. Procured items important to safety shall be qualified as being compliant with safety requirements The qualification of procured items shall include a hazard analysis to determine if there are any new hazards introduced by the use of the item

152	6	3.3.1. Proven engineering practices	Principle: Nuclear power technology is based on engineering practices that are proven by testing and experience, and which are reflected in approved codes and standards and other appropriately documented statements.	69. Systems and components are conservatively designed, constructed and tested to quality standards commensurate with the safety objectives. Approved codes and standards are used whose adequacy and applicability have been assessed and which have been supplemented or modified if necessary. If opportunities for advancement or improvement over existing practices are available and seem appropriate, such changes are applied cautiously and subjected to necessary testing. 70. Numerous codes and standards have been adopted for application in nuclear power plants, after formulation by the professional engineering community and approval by the appropriate agencies. Some existing codes and standards have been modified from their original form to take into account unique features of their use for nuclear plants and the elevated importance assigned to the safety of nuclear plants. Approved codes have the simultaneous objectives of reliability and safety. They are based on principles proven by research, past application, testing and dependable analysis. 71. Well established methods of manufacturing and construction are used. Dependence on experienced and approved suppliers contributes to confidence in the performance of important components. Deviations from previously successful manufacturing and construction practices are approved only after demonstration that the alternatives meet the requirements. Manufacturing and construction quality is ensured through the use of appropriate standards and by the proper selection, training and qualification of workers. The use of proven engineering continues throughout the plant's lifetime. When repairs and modifications are made, an analysis is conducted and a review is made to ensure that the system is returned to a configuration covered in the safety analysis and technical specifications. Where new and unreviewed safety questions are posed, a new analysis is conducted. 72. The construction techniques used for nuclear plants are applied in recognition of the critical safety issues in the plant design and accommodate them prior to commencement of physical construction. The construction aspects and techniques are also taken into consideration in the plant design in order to eliminate the need for changes in the design during construction. These considerations are an integral part of the approval process by operating organizations and regulatory authorities. 73. The design and construction of new types of power plants are based as far as possible on experience from earlier operating plants or on the results of research programmes and the operation of prototypes of an adequate size. 74. Standardization can offer economic advantages in both design and operation, and may provide some potential, indirect safety advantages by concentrating the resources of designers, regulators and manufacturers on specific design and fabrication methods. The advantages include more standardized siting requirements and engineering documentation for a set of plants. Also, standardization, if properly implemented, can promote more efficient operation, and thus safety, by direct sharing of operating experience and common training; and it can lead to more effective construction and quality assurance programmes. However, there is also a risk that standardization may lead to generic problems. This risk is reduced by adopting the concept of evolutionary improvements in the design of standardized plants.	Systems or components do not satisfy their safety requirements in a highly reliable manner.	Conservative design, construction and testing practices commensurate with safety objectives Compliance with appropriate codes and standards Proven methods of manufacturing and construction

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
191	6	4.3.2. Achievement of quality	Principle: The plant manufacturers and constructors discharge their responsibilities for the provision of equipment and construction of high quality by using well proven and established techniques and procedures supported by quality assurance practices.	250. The supply of equipment manufactured and constructed satisfactorily according to specification is an immediate responsibility of the plant manufacturer, whose success in this regard depends on the effectiveness of its practices and procedures and the way it adheres to them. Manufacturing and construction are guided by detailed specifications for processes and products, and for methods of testing and inspection. Equipment manufacturers are chosen who have demonstrated their capabilities in meeting the special and exacting requirements for nuclear power plants, which are often specific to the nuclear industry and which are based on codes and standards containing acceptance criteria for the final work products. Suppliers of important safety related equipment often have their competence checked and certified by third parties. 251. The manufacturer establishes procedures for the control of processes and documents; identification and control of materials and components; setting of inspection and test schedules; maintenance of records, hold points and corrective procedures for deviations; the whole being subject to a hierarchy of quality assurance practices. The manufacturer is responsible for the development and validation of its manufacturing practices and quality control methods, for staff training and for providing satisfactory working conditions. 252. Although the manufacturer has immediate responsibility for the quality of the equipment and plant supplied, the operating organization discharges its general responsibility for the safety of the plant by setting up arrangements within its own company, or by using organizations acting on its behalf, to review and audit the practices and documentation of the manufacturers and contractors, including quality assurance practices and organization. For important safety related items, these arrangements are available for review by regulatory authorities.	Inadequate specification for safety related equipment Inadequate procedures established by the manufacturer of safety related equipment Non-compliance of manufacturer of safety related equipment to its quality procedures	Clear, complete and correct specifications for safety related equipment Established procedures for the manufacture and construction of safety related equipment that are consistent with industry best practice Adequate review and audit of manufacturing and construction of safety related equipment
193	6	4.4.2. Validation of operating and functional test procedures	Principle: Procedures for normal plant and systems operation and for functional tests to be performed during the operating phase are validated as part of the commissioning programme.	259. Procedures to be followed during the operating phase are written before and during commissioning on the basis of information supplied by the designer and the manufacturers. Advantage is taken of the commissioning phase to test and update these operating procedures for the plant and its systems, to check out the methods that will later be used in functional testing of equipment related to safety, and in general to exercise the plant. The plant simulator is used to validate operating functional testing procedures. This activity also gives the operating staff essential preparation and training, familiarizing them with locations of systems, system responses, system peculiarities and system interactions. It is one of the principal reasons for involving the plant operating staff in commissioning activities at an early stage.	Inadequate operating procedures to maintain the plant within the safe operating envelope	Clear, complete and correct operating procedures that have been validated during the commissioning phase
194	6	4.4.3. Collecting baseline data	Principle: During commissioning tests, detailed diagnostic data are collected on components having special safety significance and the initial operating parameters of the systems are recorded.	261. Baseline data are collected during commissioning and early operation as reference points to assist in later surveillance for the detection of incipient degradation of the plant components. Included in this process are the fundamentally important inspections and tests of the reactor pressure vessels and other primary component boundaries. In general, baseline data are collected during commissioning for all safety related parameters that are to be routinely measured and monitored during operation.	Degradation of performance of safety related equipment is not detected due to lack of baseline data for comparison	Collection of baseline data of the performance of safety related equipment during commissioning that will be used as a basis of comparison during the operating life of the plant

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
195	6	4.4.4. Pre-operational plant adjustments	Principle: During the commissioning programme, the as-built operating characteristics of safety and process systems are determined and documented. Operating points are adjusted to conform to design values and to safety analyses. Training procedures and limiting conditions for operation are modified to reflect accurately the operating characteristics of the systems as built.	263. Process and safety systems are tested and calibrated during the pre-operational period. The information obtained indicates where adjustments are needed to ensure that the plant, the plant simulator, the safety analysis, operating staff training and operating procedures conform to a unified basis. In this way, the plant is made to work in the intended fashion when it is brought to the normal operating state.	Operating envelope definition is not modified to reflect as-built performance of the safety related plant equipment	Update the safe operating envelope definition and related operating procedures to reflect the as-built performance of safety related equipment

DESIGN AND CONSTRUCTION PHASE

Organization

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
33	3	Requirement 3: Responsibility of senior management for the management system	Senior management shall be responsible for establishing, applying, sustaining and continuously improving a management system to ensure safety.	4.1. Senior management shall retain accountability for the management system even where individuals are assigned responsibility for coordinating the development, application and maintenance of the management system [1, 2]. 4.2. Senior management shall be responsible for establishing safety policy.	Lack of Adequately Defined and Executed Safety Management Plan	Clear accountability for the establishment of a safety management system

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
39	3	Requirement 9: Provision of resources	Senior management shall determine the competences and resources necessary to carry out the activities of the organization safely and shall provide them.	4.21. Senior management shall make arrangements to ensure that the organization has in-house, or maintains access to, the full range of competences and the resources necessary to conduct its activities and to discharge its responsibilities for ensuring safety at each stage in the lifetime of the facility or activity, and during an emergency response [13, 14, 18].10 4.22. Senior management shall determine which competences and resources the organization has to retain or has to develop internally, and which competences and resources may be obtained externally, for ensuring safety. 4.23. Senior management shall ensure that competence requirements for individuals at all levels are specified and shall ensure that training is conducted, or other actions are taken, to achieve and to sustain the required levels of competence. An evaluation shall be conducted of the effectiveness of the training and of the actions taken. 4.24. Competences to be sustained in-house by the organization shall include: competences for leadership at all management levels; competences for fostering and sustaining a strong safety culture; and expertise to understand technical, human and organizational aspects relating to the facility or the activity in order to ensure safety. 4.25. Senior management shall ensure that individuals at all levels, including managers and workers: (a) Are competent to perform their assigned tasks and to work safely and effectively; (b) Understand the standards that they are expected to apply in completing their tasks. 4.26. All individuals in the organization shall be trained in the relevant requirements of the management system. Such training shall be conducted to ensure that individuals are knowledgeable of the relevance and the importance of their activities and of how their activities contribute to ensuring safety in the achievement of the organization’s goals. 4.27. The knowledge and the information of the organization shall be managed as a resource.	Lack of Competent Personnel	Competencies required for each design activity are clearly defined The management system shall ensure that personnel assigned to design activities have the pre-requisite competencies to perform those activities

DESIGN AND CONSTRUCTION PHASE

Governance

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
29	1	Requirement 1: Responsibilities in the management of safety in plant design	An applicant for a licence to construct and/or operate a nuclear power plant shall be responsible for ensuring that the design submitted to the regulatory body meets all applicable safety requirements.	3.1. All organizations, including the design organization, engaged in activities important to the safety of the design of a nuclear power plant shall be responsible for ensuring that safety matters are given the highest priority.	Not Taking Safety into Account in Decision Making	Well documented expectations for the design process Design process consistent with industry best practice Well documented competencies required for the performance of each design process Documented assessments of personnel demonstrating required competencies for tasks/processes assigned to them Adequate schedule and resources provided to perform design processes in accordance with expectations
30	3	Requirement 1: Achieving the fundamental safety objective	The registrant or licensee — starting with the senior management — shall ensure that the fundamental safety objective of protecting people and the environment from harmful effects of ionizing radiation is achieved.	2.1. The registrant or licensee shall ensure that provisions are made to achieve the fundamental safety objective. 2.2. The senior management of organizations, in accordance with their accountabilities: (a) Shall ensure the safe siting, design, construction, commissioning, operation and decommissioning (or closure) of facilities [2, 9, 11–14]; (b) Shall ensure that equipment and activities meet safety standards, quality standards and management standards; (c) Shall ensure the safe management and control of all radioactive material and radiation sources that are produced, processed, used, handled, transported, stored or disposed of [5, 15]; (d) Shall ensure that managers at all levels in the organization develop and maintain an understanding of radiation risks and potential consequences, and of how to manage radiation risks relevant to their responsibilities [16]; (e) Shall ensure that provision is made for adequate resources and funding, including for the long term management and disposal of radioactive waste, as well as for decommissioning (or closure) of facilities, with due consideration given to the protection of future generations [9, 15, 17]; (f) Shall ensure that adequate arrangements are made where appropriate for preparedness and response for a nuclear or radiological emergency [18, 19].	Lack of Adequately Defined and Executed Safety Management Plan	Documented safety management plan Compliance of safety management plan with industry standards Understanding of all personnel on their role in the safety management plan Assessments and audits of compliance with safety management plan

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
31	3	Requirement 12: Fostering a culture for safety	Individuals in the organization, from senior managers downwards, shall foster a strong safety culture. The management system and leadership for safety shall be such as to foster and sustain a strong safety culture.	5.1. All individuals in the organization shall contribute to fostering and sustaining a strong safety culture [1, 2]. 5.2. Senior managers and all other managers shall advocate and support the following: (a) A common understanding of safety and of safety culture, including: awareness of radiation risks and hazards relating to work and to the working environment; an understanding of the significance of radiation risks and hazards for safety; and a collective commitment to safety by teams and individuals; (b) Acceptance by individuals of personal accountability for their attitudes and conduct with regard to safety; (c) An organizational culture that supports and encourages trust, collaboration, consultation and communication; (d) The reporting of problems relating to technical, human and organizational factors and reporting of any deficiencies in structures, systems and components to avoid degradation of safety, including the timely acknowledgement of, and reporting back of, actions taken; (e) Measures to encourage a questioning and learning attitude at all levels in the organization and to discourage complacency with regard to safety; (f) The means by which the organization seeks to enhance safety and to foster and sustain a strong safety culture, and using a systemic approach (i.e. an approach relating to the system as a whole in which the interactions between technical, human and organizational factors are duly considered); (g) Safety oriented decision making in all activities; (h) The exchange of ideas between, and the combination of, safety culture and security culture.	Lack of Strong Safety Culture	Responsibilities are well known and understood in a safety policy statement. Adequate resources are devoted to safety. All organizations arrange for regular review of their practices that contribute to nuclear plant safety. Managers at the most senior level demonstrate their commitment by their attention to regular review of the processes that bear on nuclear safety, by taking direct interest in the more significant questions of nuclear safety or product quality as they arise, and by frequent citation of the importance of safety and quality in communications to staff. Managers ensure that work on matters related to nuclear safety is carried out in a rigorous manner. Managers ensure that their staff are fully competent for their duties. Managers encourage and praise and seek to provide tangible reward for particularly commendable attitudes in safety matters. Managers make arrangements to benefit from all sources of relevant experience, research, technical developments, operational data and events of safety significance, all of which are carefully evaluated in their own contexts. Individuals recognize that a communicative approach is essential to safety.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
32	3	Requirement 2: Demonstration of leadership for safety by managers	Managers shall demonstrate leadership for safety and commitment to safety.	3.1. The senior management of the organization shall demonstrate leadership for safety by: (a) Establishing, advocating and adhering to an organizational approach to safety that stipulates that, as an overriding priority, issues relating to protection and safety receive the attention warranted by their significance; (b) Acknowledging that safety encompasses interactions between people, technology and the organization [2]; (c) Establishing behavioural expectations and fostering a strong safety culture; (d) Establishing the acceptance of personal accountability in relation to safety on the part of all individuals in the organization and establishing that decisions taken at all levels take account of the priorities and accountabilities for safety. 3.2. Managers at all levels in the organization, taking into account their duties, shall ensure that their leadership includes: (a) Setting goals for safety that are consistent with the organization's policy for safety, actively seeking information on safety performance within their area of responsibility and demonstrating commitment to improving safety performance; (b) Development of individual and institutional values and expectations for safety throughout the organization by means of their decisions, statements and actions; (c) Ensuring that their actions serve to encourage the reporting of safety related problems, to develop questioning and learning attitudes, and to correct acts or conditions that are adverse to safety. 3.3. Managers at all levels in the organization: (a) Shall encourage and support all individuals in achieving safety goals and performing their tasks safely; (b) Shall engage all individuals in enhancing safety performance; (c) Shall communicate clearly the basis for decisions relevant to safety.	Not Taking Safety into Account in Decision Making	Clearly established policy and governance with respect to the expectations for taking safety into account in all decisions Clearly established expectations on the leadership to communicate, demonstrate and reinforce the expected safety behaviour
34	3	Requirement 4: Goals, strategies, plans and objectives	Senior management shall establish goals, strategies, plans and objectives for the organization that are consistent with the organization's safety policy.	4.3. Goals, strategies, plans and objectives for the organization shall be developed in such a manner that safety is not compromised by other priorities. 4.4. Senior management shall ensure that measurable safety goals that are in line with these strategies, plans and objectives are established at various levels in the organization. 4.5. Senior management shall ensure that goals, strategies and plans are periodically reviewed against the safety objectives, and that actions are taken where necessary to address any deviations.	Not Taking Safety into Account in Decision Making	Clear and measurable safety goals are established at various levels in the organizations Expectation that safety goals are periodically reviewed against organizational strategies and plans are established

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
35	3	Requirement 5: Interaction with interested parties	Senior management shall ensure that appropriate interaction with interested parties takes place.	4.6. Senior management shall identify interested parties for their organization and shall define an appropriate strategy for interaction with them. 4.7. Senior management shall ensure that the processes and plans resulting from the strategy for interaction with interested parties include: (a) Appropriate means of communicating routinely and effectively with and informing interested parties with regard to radiation risks associated with the operation of facilities and the conduct of activities; (b) Appropriate means of timely and effective communication with interested parties in circumstances that have changed or that were unanticipated; (c) Appropriate means of dissemination to interested parties of necessary information relevant to safety; (d) Appropriate means of considering in decision making processes the concerns and expectations of interested parties in relation to safety.	Not Taking Safety into Account in Decision Making	Expectation for effective communications and interactions with interested parties about safety is established

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
36	3	Requirement 6: Integration of the management system	The management system shall integrate its elements, including safety, health, environmental, security, quality, human-and-organizational-factor, societal and economic elements, so that safety is not compromised.	4.8. The management system shall be developed, applied and continuously improved. It shall be aligned with the safety goals of the organization. 4.9. The management system shall be applied to achieve goals safely, to enhance safety and to foster a strong safety culture by: (a) Bringing together in a coherent manner all the necessary elements for safely managing the organization and its activities; (b) Describing the arrangements made for management of the organization and its activities; (c) Describing the planned and systematic actions necessary to provide confidence that all requirements are met; (d) Ensuring that safety is taken into account in decision making and is not compromised by any decisions taken. 4.10. Arrangements shall be made in the management system for the resolution of conflicts arising in decision making processes. Potential impacts of security measures on safety and potential impacts of safety measures on security shall be identified and shall be resolved without compromising safety or security [20–23]. 4.11. The organizational structures, processes, responsibilities, accountabilities, levels of authority and interfaces within the organization and with external organizations shall be clearly specified in the management system. 4.12. Regulatory requirements shall be reflected in the management system. 4.13. Provision shall be made in the management system to identify any changes (including organizational changes and the cumulative effects of minor changes) that could have significant implications for safety and to ensure that they are appropriately analysed. 4.14. Arrangements shall be established in the management system for an independent review to be made before decisions significant for safety are made. The requirements on the independent nature of the review and on the necessary competences of the reviewers shall be specified in the management system.	Lack of Adequately Defined and Executed Safety Management Plan	Expectations that the safety management system be developed, applied and continuously improved shall be established. The safety management system shall be integrated into the overall management system
37	3	Requirement 7: Application of the graded approach to the management system	The management system shall be developed and applied using a graded approach.	4.15. The criteria used to grade the development and application of the management system shall be documented in the management system. The following shall be taken into account: (a) The safety significance and complexity of the organization, operation of the facility or conduct of the activity; (b) The hazards and the magnitude of the potential impacts (risks) associated with the safety, health, environmental, security, quality and economic elements of each facility or activity [16, 24–26]; (c) The possible consequences for safety if a failure or an unanticipated event occurs or if an activity is inadequately planned or improperly carried out.	Not Taking Safety into Account in Decision Making	Criteria are established to grade the development and application of the management system taking into account the safety significance of decisions

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
38	3	Requirement 8: Documentation of the management system	The management system shall be documented. The documentation of the management system shall be controlled, usable, readable, clearly identified and readily available at the point of use.	4.16. The documentation of the management system shall include as a minimum: policy statements of the organization on values and behavioural expectations; the fundamental safety objective; a description of the organization and its structure; a description of the responsibilities and accountabilities; the levels of authority, including all interactions of those managing, performing and assessing work and including all processes; a description of how the management system complies with regulatory requirements that apply to the organization; and a description of the interactions with external organizations and with interested parties. 4.17. Documents shall be controlled. All individuals responsible for preparing, reviewing, revising and approving documents shall be competent to perform the tasks and shall be given access to appropriate information on which to base their input or decisions. 4.18. Revisions to documents shall be controlled, reviewed and recorded. Revised documents shall be subject to the same level of approval as the initial documents. 4.19. Records shall be specified in the management system and shall be controlled. All records shall be readable, complete, identifiable and easily retrievable. 4.20. Retention times of records and associated test materials and specimens shall be established to be consistent with the statutory requirements and with the obligations for knowledge management of the organization. The media used for records shall be such as to ensure that the records are readable for the duration of the retention times specified for each record.	Lack of Adequately Defined and Executed Safety Management Plan	Establishment of clear expectations on the documentation, revisions control and communication of the safety management system
161	6	4.1.1. External factors affecting the plant	Principle: The choice of site takes into account the results of investigations of local factors that could adversely affect the safety of the plant.	137. Local factors include natural factors and human made hazards. Natural factors to be considered include geological and seismological characteristics and the potential for hydrological and meteorological disturbances. Human made hazards include those arising from chemical installations, the release of toxic and flammable gases, and aircraft impact. The investigations required give information on the likelihood of significant external events and their possible effects on nuclear power plant safety. This is developed in the form of quantified probabilities when possible. The corresponding risk evaluation takes into account the safety features provided by the design to cope with these events. Special attention is given to the potential for extreme external events and to the feasibility of installing compensating safety features.		Principle: Normal operation and anticipated operational occurrences are controlled so that plant and system variables remain within their operating ranges. This reduces the frequency of demands on the safety systems.
162	6	4.1.2. Radiological impact on the public and the local environment	Principle: Sites are investigated from the standpoint of the radiological impact of the plant in normal operation and in accident conditions.	139. Air, food-chains and water supplies provide pathways for the possible transport of radioactive material to humans. Site characteristics to be investigated are those 40 which can influence the pathways: physical characteristics such as topography, meteorology and hydrology; environmental characteristics such as type of vegetation and animal life; the use of land and water resources; and the population distribution around the site. The results of these investigations are used to demonstrate that the safety objectives are fulfilled, in normal operation with appropriate limits on effluent discharges, and for accidental radioactive releases with provisions for off-site countermeasures taken into account.		Principle: A set of operational limits and conditions is defined to identify safe boundaries for plant operation. Minimum requirements are also set for the availability of staff and equipment.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
163	6	4.1.3. Feasibility of emergency plans	Principle: The site selected for a nuclear power plant is compatible with the offsite countermeasures that may be necessary to limit the effects of accidental releases of radioactive substances, and is expected to remain compatible with such measures.	141. In a later section on emergency planning (Section 4.8.1), there are discussions of measures for which preparation is made to cope with very improbable accidents that could affect public health and the environment. The feasibility of such emergency plans may be affected by features of the site and its surroundings, and this is taken into account in the initial site review. For future nuclear power plants, the protective emergency measures could be reduced in terms of both area of coverage and time of application in recognition of the objectives set in paras 25 and 27.	Offsite countermeasures required to limit the effects of accidental releases of radioactive substances are not in place.	Principle: Plant management institutes measures to ensure that events significant for safety are detected and evaluated in depth, and that any necessary corrective measures are taken promptly and information on them is disseminated. The plant management has access to operational experience relevant to plant safety from other nuclear power plants around the world.
164	6	4.1.4. Ultimate heat sink provisions	Principle: The site selected for a nuclear power plant has a reliable long term heat sink that can remove energy generated in the plant after shutdown, both immediately after shutdown and over the longer term.	143. In some cases, extreme conditions in such events as earthquakes, floods and tornadoes could threaten the availability of the ultimate heat sink unless adequate design precautions are taken. The choice of the atmosphere as an ultimate heat sink is acceptable, provided that the design ensures that the heat removal system would withstand any extreme event that must be taken into account.	A long term heat sink for removal of energy after a shutdown is not reliably available.	Principle: The results of an analysis of the response of the plant to potential accidents beyond the design basis are used in preparing guidance on an accident management strategy.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
166	6	4.2.1.2. Proven technology	Principle: Technologies incorporated into design have been proven by experience and testing. Significant new design features or new reactor types are introduced only after thorough research and prototype testing at the component, system or plant level, as appropriate.	155. This principle is a specific application of the fundamental principle of Section 3.3.1 to nuclear power plant design. Disciplined engineering practice requires a balance between technological innovation and established engineering practices. Design is in accordance with applicable national or international standards, particularly those developed specifically for nuclear use, which are accepted by the professional engineering community and recognized by the appropriate national or international institutions. These standards reflect engineering practices proven in past use. It is nevertheless always necessary to allow for consideration of the need for, and the value of, improvements beyond established practice. These are first brought to the level of 'proven engineering' through appropriate testing and scaling up if needed. 156. An example of this balance between proven technology and technological innovation is the recent interest in and broad application of passive safety features. The advantages and disadvantages of these passive features are carefully considered in the design process. The essential advantages of passive features are their independence from external support systems such as electric power, their generally greater simplicity and their potential for increased reliability. Disadvantages include lower driving heads in fluid systems and reduced flexibility in abnormal conditions. Furthermore, special attention has to be paid to limitations in the existing data on the performance of new passive systems and adequate experimental and analytical verification of their performance is necessary. Finally, active components may still be necessary for startup and shutdown. 157. Most application of engineering technology requires the use of analytical methods. The physical and mathematical models used in design are validated by means of experimental or operational testing and analysis of data. Results of more complex analysis are verified by pertinent experimentally based benchmark calculations, type testing and peer review. Where possible, realistic modelling and data are used to predict plant performance, safety margins and the evolution of accident conditions. Where realistic modelling is not feasible, conservative models are used.	System or components that are related to implemented safety related functions are not reliable.	Technologies incorporated into design have been proven by experience and testing. Significant new design features or new reactor types are introduced only after thorough research and prototype testing at the component, system or plant level, as appropriate.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
167	6	4.2.1.3. General basis for design	A nuclear power plant is designed to cope with a set of events including normal conditions, anticipated operational occurrences, extreme external events and accident conditions. For this purpose, conservative rules and criteria incorporating safety margins are used to establish design requirements. Comprehensive analyses are carried out to evaluate the safety performance or capability of the various components and systems in the plant.	159. The various events that the plant has to accommodate are classified according to their probabilities of occurrence. Attention in design ensures that there is no damage to the plant as a result of events classed as normal operating events, or for which there is a reasonable expectation of occurrence during the lifetime of the plant. At a much lower level of probability are combinations of human and mechanical failure that could jeopardize the protection provided by inherent plant features and normal plant systems. 160. Engineered safety systems are included in plant design, as discussed in Section 3.3, to protect against the possibility of occurrence of classes of accidents that would otherwise contribute significantly to risk, or to mitigate the consequences of such accidents. Design assessments of engineered safety systems will provide assurance that there are no cross-linked interactions with other independent systems which could detrimentally impact their performance. Any engineered safety system is designed to prevent or to mitigate a specific spectrum of accidents. The accidents in this spectrum that tax the features of the safety system most are termed the design basis accidents for that system. The plant and the engineered safeguards are so designed that none of these accidents or accident sequences dominates the total risk. In design, attention is given to requirements for such future activities as maintenance and periodic testing, to ensure continued conformity to the principle. 161. All components, structures and systems can be classified on the basis of their function and significance for safety to provide a basis for determining the appropriate codes, standards and other requirements to be applied in their design, construction, installation, operation, maintenance, environmental qualification and inspection. 162. For future nuclear power plants, realistic assumptions and best estimate analyses are used to assess the additional multiple failures and severe core damage sequences considered in the design process.	Design requirements for safety related functions do not reflect adequately conservative decision making.	Designed to cope with a set of events including normal conditions, anticipated operational occurrences, extreme external events and accident conditions. For this purpose, conservative rules and criteria incorporating safety margins are used to establish design requirements. Comprehensive analyses are carried out to evaluate the safety performance or capability of the various components and systems in the plant.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
169	6	4.2.2.2. Automatic safety systems	Principle: Automatic systems are provided that would safely shut down the reactor, maintain it in a shut down and cooled state, and limit any release of fission products that might possibly ensue, if operating conditions were to exceed predetermined set points.	169. Despite the high quality of the design and construction and any self-controlling features of the plant, it is anticipated that sequences of events originating either inside or outside the plant will occasionally occur that exceed the protective capabilities of normal plant control systems. These hypothetical failures constitute a broad range of initiators of accidents against which the design is evaluated. Engineered safety features are incorporated as necessary to ensure that plant damage, especially damage to the reactor core, would be limited even in the most severe of these design basis accidents. In such circumstances, reactor power would be controlled, core cooling would be maintained and any radioactive material released from the fuel would remain confined by suitable physical barriers. 170. Stringent requirements preclude bypassing automatic safety systems. In current and future plants, consideration is given to improving safety systems in terms of reliability and response time. 171. Initiation and operation of the engineered safety features are highly reliable. This reliability is achieved by: the appropriate use of fail-safe design; by protection against common cause failures; and by independence between safety systems and plant process systems. The design of these systems ensures that failure of a single component would not cause loss of the function served by a safety system (the single failure criterion). Where a system is relied upon to perform both safety and process functions, special consideration is given to ensuring that the safety function is not affected by expected or inadvertent process control demands. 172. Proven engineering practice, operating experience and safety analysis call for high reliability of electrical and instrumentation systems supporting safety systems. Many of the mechanical and fluid systems that shut down the reactor, cool the fuel or confine the radioactive materials depend upon electricity to power their active components, indicate their status and control their operation. Thus, the reliability of safety systems is determined by the reliability of the electrical, fluid and instrumentation systems that support them. In the event of the modernization and/or refurbishment of instrumentation and control (I&C) systems important to safety in operating nuclear power plants, it is necessary to consider the interfaces to existing devices and environmental conditions such as those relating to the power supply, auxiliary equipment and electromagnetic interference (EMI). 173. Plant design includes the capability to test automatic safety systems throughout the plant's lifetime, with automatic self-tests where possible. Test conditions seek to reproduce operating conditions.	Requirements for plant control systems do not handle all sequences of events that can lead to an accident. Requirements for safety systems do not address all sequences of events that can lead to an accident. Implementation of control and safety systems are not commensurate with their reliability requirements.	Automatic systems are provided that would safely shut down the reactor, maintain it in a shut down and cooled state, and limit any release of fission products that might possibly ensue, if operating conditions were to exceed predetermined set points.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
170	6	4.2.2.3. Reliability targets	Principle: Reliability targets are assigned to safety systems or functions. The targets are established on the basis of the safety objectives and are consistent with the roles of the systems or functions in different accident sequences. Provision is made for testing and inspection of components and systems for which reliability targets have been set.	175. Generally applicable design requirements for high reliability of safety systems and functions are translated into specific reliability targets. The reliability of support services required for the operation of safety systems or functions, such as electrical power or cooling water, is considered in the formulation of reliability targets. Appropriate reliability targets are set to ensure performance on demand and operation throughout the required duration of performance. These targets are based on engineering analysis. Detailed probabilistic methods are useful in determining the reliability required of safety systems and functions. Regardless of how the reliability targets are established, a reliability analysis is conducted during the design process to ensure that safety systems and functions can meet them. Functional testing and system modelling are used to demonstrate that the reliability targets will continue to be met during plant service. The need for continued assurance of reliability during operation places a requirement on the designer to provide systems which are testable in service, under realistic demand and performance conditions if possible. 176. For some systems, reliability targets may exceed values that can be demonstrated. If it is necessary to ensure this greater functional reliability, additional independent systems are used, each of which is capable of performing the assigned safety function. Diversity and physical separation of these systems reduce the possibility of common mode failures.	Reliability targets are either not established for safety systems or are established inconsistent with achieving the safety goals of the plant. Design and implementation of safety system does not satisfy reliability targets. Diversity is not adequately implemented in the design of safety systems in cases where achievement of the reliability target cannot be demonstrated.	Reliability targets are assigned to safety systems or functions. The targets are established on the basis of the safety objectives and are consistent with the roles of the systems or functions in different accident sequences. Provision is made for testing and inspection of components and systems for which reliability targets have been set.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
171	6	4.2.2.4. Dependent failures	Principle: Design provisions seek to prevent the loss of safety functions due to damage to several components, systems or structures resulting from a common cause.	178. The appropriate design method to prevent damage to two or more systems simultaneously is determined by specific circumstances. Among the methods used are physical separation by barriers or distance, protective barriers, redundancy linked with diversity and qualification to withstand the damage. 179. Some common cause events that must be considered would have their origins in occurrences internal to the plant. These include the loss of common electrical power sources, depletion of fuel for diesel generators, loss of common service functions, fire, explosion, flooding, projectiles ejected in the failure of rotating or pressurized components, system interaction, or error in design, operation, maintenance or testing. Failures due to undetected flaws in manufacturing and construction are also considered. Common cause events external to the plant include natural events such as earthquakes, high winds and floods, as well as such human made hazards as aircraft crashes, drifting explosive clouds, fires and explosions, which could originate from other activities not related to the nuclear power plant. For a site with more than one reactor unit, events that could originate in the units on the site are considered as additional external initiating events for the other units. 180. Because of the importance of fire as a source of possible simultaneous damage to several components, design provisions to prevent and combat fires in the plant are given special attention. Fire resistant materials are used to the extent possible. Firefighting capability is included in the design specifications. Lubrication systems use non-flammable lubricants or are protected against the initiation and the effects of fires. The design takes advantage of the methods identified for preventing common cause failures. 181. Of the extreme external hazards, seismic events receive special attention owing to the extent to which they can jeopardize safety. A nuclear power plant is protected against earthquakes in two ways: by siting it away from areas of active faulting and related potential problems such as susceptibility to soil liquefaction or landslides; and by designing the physical barriers and the safety systems contributing to the defence in depth of the plant to bear the vibratory loads associated with the most severe earthquake that could be expected to occur in its vicinity, on the basis of historical input and tectonic evidence. This is termed the design basis earthquake. Seismic design of plant structures, components and systems is carried out using response function methods, making use of a frequency spectrum for the design basis earthquake that is appropriate to the site. Seismic design takes account of soil–structure interaction, the potential amplification and modification of seismic motion by the plant structures, and interaction between components, systems and structures. The design ensures that the failure of non-safety-related equipment in an earthquake would not affect the performance of safety equipment.	Inadequate design in terms of redundancy, independence, separation and diversity to avoid common cause failures that result in the loss of one or more safety functions.	Design provisions seek to prevent the loss of safety functions due to damage to several components, systems or structures resulting from a common cause.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
172	6	4.2.2.5. Equipment qualification	Principle: Safety components and systems are chosen that are qualified for the environmental conditions that would prevail if they were required to function. The effects of ageing on normal and abnormal functioning are considered in design and qualification.	183. The conditions under which equipment is required to perform a safety function may differ from those to which it is normally exposed, and its performance may be affected by ageing or by service conditions as plant operation goes on. The environmental conditions under which equipment is required to function are identified as part of the design process. Among these are the conditions expected in a wide range of accidents, including extremes of temperature, pressure, radiation, vibration, humidity and jet impingement, including their interactions, as well as severe accidents for future nuclear power plants, consistent with the objectives set out in para. 25. The effects of external events such as earthquakes are also considered. 184. The required reliability is to be maintained throughout the plant's lifetime. Attention is given during design to the common cause failure effects of ageing and to the effects of ageing on the plant's capacity to withstand the environmental effects of accidents considered in the design. Ageing is taken account of in the design by the appropriate specification of environmental conditions, process conditions, duty cycles, maintenance schedules, service lifetime, type testing schedules, replacement parts and replacement intervals. 185. It is preferable that qualification be achieved by the testing of prototypical equipment. This is not always fully practicable for the vibration testing of large components or the ageing of equipment. In such cases, analysis or tests plus analyses are relied upon.	Safety systems do not deliver required functionality in all environmental conditions that the equipment would be subject to during an accident. The effects of ageing are not adequately considered in the design resulting in eventual loss of some safety functions.	Safety components and systems are chosen that are qualified for the environmental conditions that would prevail if they were required to function. The effects of ageing on normal and abnormal functioning are considered in design and qualification.
173	6	4.2.2.6. Inspectability of safety equipment	Principle: Safety related components, systems and structures are designed and constructed so that they can be inspected throughout their operating lifetimes to verify their continued acceptability for service with an adequate safety margin.	187. In-service inspection is relied upon to demonstrate that safety provisions are maintained throughout the lifetime of the plant. Provision is made at the design stage for inspection access, and for the ease and frequency of inspection. In-service inspection of the primary coolant system boundary receives special attention because of the great reliance placed upon coolant retention and the environmental conditions to which the primary system boundary is exposed for a long period of time. The radiological protection of workers is also carefully considered in designing for the in-service inspection of safety equipment. Other safety systems that receive attention in design to ensure their inspectability include electrical cable runs, junction boxes, penetrations of the confinement system boundary, coolant and lubrication systems, and components including organic materials and other materials that may degrade with age or as a result of radiation exposure.	Safety system fails to deliver one or more safety functions due to ageing of some safety system components.	Safety related components, systems and structures are designed and constructed so that they can be inspected throughout their operating lifetimes to verify their continued acceptability for service with an adequate safety margin.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
174	6	4.2.2.7. Radiation protection in design	Principle: At the design stage, radiation protection features are incorporated to protect plant personnel from radiation exposure and to keep emissions of radioactive effluents within prescribed limits.	189. Designers provide for protection of the operating and maintenance staff from direct exposure to radiation and from contamination by radioactive material. Care is taken in the design of radioactive waste systems to provide for conservative adherence to authorized limits. The design ensures that all plant components containing radioactive material are adequately shielded and that the radioactive material is suitably contained. This protection is effective in routine operations, and is also helpful in nonroutine circumstances such as during maintenance and engineering modification, when activities are more varied. Design of the plant layout takes into account radiation protection requirements, by attention to the appropriate location of plant components and systems, shielding requirements, confinement of radioactive materials, accessibility, access control, the need for monitoring and control of the working environment, and decontamination. Consideration is given to the use of materials which do not become exceptionally radioactive with long half-lives under neutron irradiation; to the avoidance of design features which promote the retention of activated material in locations from which it can be removed only with difficulty; and to the use of surface finishes which facilitate decontamination. Facilities for personnel and area monitoring and personnel decontamination are included in the plant design. 190. Attention is also paid at the design stage to radiological protection in the decommissioning phase. After the end of the operating lifetime of the plant, and after the removal of all nuclear fuel, substantial amounts of radioactive material will remain on the site. Consideration is given to the choice of materials which will have low residual activity on the time-scale important for decommissioning, and to the need for convenient access for dismantling.	Plant design does not adequately take into account protection of operating and maintenance staff.	Radiation protection features are incorporated to protect plant personnel from radiation exposure and to keep emissions of radioactive effluents within prescribed limits.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
175	6	4.2.3.1. Protection against power transient accidents	Principle: The reactor is designed so that reactivity induced accidents are protected against, with a conservative margin of safety.	193. A reactivity induced accident would be one in which an increase in reactivity occurred, either globally or locally, causing the reactor power to exceed the heat removal rate and thus to damage the fuel. Two features of a nuclear plant are important in counteracting such an increase in reactivity. One is negative reactivity feedback, and the other is the system which introduces a neutron absorber or reduces the reactivity by some other means, to compensate for the reactivity increase or to curtail power generation. Both features are influenced by design choices. Negative reactivity feedback coefficients alone cannot prevent all conceivable reactivity induced accidents or damage due to such accidents, but they can be effective in doing this in many cases, through their stabilizing effects. Therefore, the design of a reactor core usually relies in part on such inherent features to assist in preventing reactivity induced accidents. Where inherent characteristics alone cannot prevent reactivity induced accidents, control systems are designed to ensure reliable reactivity control under all operating conditions. The safety shutdown system is designed to have the reliability and effectiveness necessary for the timely suppression of reactivity induced power transients and the prevention of damage to the reactor core from such a cause. The great importance of achieving this is reflected in the commensurate assurance that the combination of inherent feedback features, reactivity control systems and shutdown systems achieves its purpose with a satisfactory margin. This assurance includes an experimental and analytical demonstration that the reliability of the shutdown system is adequate, and analysis to verify also that the effects of possible transients would be tolerable. Furthermore, reliable means are provided to prevent fast (slug type) boron dilution (for pressurized water reactors). 194. Attention is given to ensuring that external events, failures of equipment or human errors would not lead to reactivity induced accidents. In addition, attention is given to the prevention of reactivity induced accidents that might result from actions originating otherwise than in the normal operation of the plant. The most important design measures to be taken are those that combine limits on withdrawal rates of shim, control and safety rods with strategies of rod management and automatic control and protection systems; to ensure that the removal or addition of a single control rod would not introduce transients that would cause significant damage to an on-line reloaded reactor core; and that a reactor being batch loaded would not become critical during the loading process. The withdrawal of any single control rod in the completely shut down reactor does not make the reactor core critical.	The design and implementation of the safety systems is inadequate to protect against reactivity induced accidents.	Design should be as inherently safe as possible Control of system should maintain the system in a safe state Mitigating system shall put system into a safe state if the control systems fail

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
176	6	4.2.3.2. Reactor core integrity	Principle: The core is designed to have mechanical stability. It is designed to tolerate an appropriate range of anticipated variations in operational parameters. The core design is such that the expected core distortion or movement during an accident within the design basis would not impair the effectiveness of the reactivity control or the safety shutdown systems or prevent cooling of the fuel.	196. Fuel rods tend to be distorted and displaced if there is a steep radial gradient of heating rate across the core of a reactor. If this is not countered, core distortion may result, possibly inducing reactivity changes or inhibiting the insertion of safety and control rods or elements. In some cases, distortion could affect the hydraulic diameters of specific channels, and hence the cooling of the fuel. Similar effects could result from radiation damage in graphite moderated reactor cores unless allowance is made to take account of the radiation induced dimensional changes in the graphite. Some precautions, such as restraints, may be necessary to prevent undesirable effects of thermal, mechanical and radiation induced distortion of the core. 197. Fuel rod vibration induced by thermal–hydraulic effects is prevented by mechanical constraint. This prevents associated neutronic fluctuations and excessive fretting and wear of cladding. Fuel assemblies and other core components are restrained so that abrupt shifts in position cannot cause sudden or large reactivity changes. Care is taken to ensure that restraints do not themselves introduce safety problems. 198. Analysis supported by suitable experiments verifies that the core is geometrically stable against potential earthquakes, system transients and other dynamic forces to which it might be subjected. 199. High quality of fuel rods is an important safety requirement. Damaged or distorted fuel can potentially inhibit cooling and the reactivity reduction process. Furthermore, cladding failure represents a basic loss of defence in depth. Less severe damage may reduce the ability of the fuel to withstand accident conditions. For these reasons, special quality assurance measures are taken in the design and manufacture of fuel. Continued fuel integrity is verified by monitoring the activity in the coolant during operation.	Reactivity control or safety shutdown system is not effective during some design basis event due to mechanical instability.	The core is designed to have mechanical stability. It is designed to tolerate an appropriate range of anticipated variations in operational parameters. The core design is such that the expected core distortion or movement during an accident within the design basis would not impair the effectiveness of the reactivity control or the safety shutdown systems or prevent cooling of the fuel.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
177	6	4.2.3.3. Automatic shutdown systems	Principle: Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent of the equipment and processes used to control the reactor power. Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally.	201. Safety shutdown systems are independent in function from the reactivity control systems used for normal operation of the reactor. Common sensors or devices may only be used if reliability analysis indicates that this is acceptable. Under all conditions taken into account in the design, when the core is critical or may become critical, safety shutdown mechanisms with sufficient negative reactivity are poised to initiate safe shutdown if required. The rate of reactivity addition is an important parameter in some accident sequences, and design steps are required to retain this parameter within appropriate limits defined by the design basis. Electrical buses and logic circuits of the shutdown system are separate from instruments used for normal control so that no interference is possible between the demands of normal control and the demands of safe shutdown. Only when the reactor is in a predefined 'guaranteed shutdown state' with sufficient subcriticality can the safety shutdown systems be safely disabled. 202. One unlikely event which must be analysed is the failure of an automatic shutdown system to act when it is called upon. The scenario is highly plant dependent, and it varies with the circumstances leading to the signal for automatic shutdown. The consequences might be an excessive increase in reactivity, an excessive primary circuit pressure, excessive fuel temperatures or some other potential cause of damage to the plant. The plant is so designed that these anticipated transients without scram (ATWS) do not contribute appreciably to risk, consistent with the technical safety objective of Section 2.3. This is achieved by making the accidents sufficiently unlikely or by ensuring that they will not lead to severe core damage. Attention to prevention of these accidents or to limitation of their effects ensures that the safety objective is met even with account taken of this failure of plant protection.	Requirements for plant control systems do not handle all sequences of events that can lead to an accident. Requirements for safety systems do not address all sequences of events that can lead to an accident. Implementation of control and safety systems are not commensurate with their reliability requirements.	Rapidly responding and highly reliable reactivity reduction for safety purposes is designed to be independent of the equipment and processes used to control the reactor power. Safety shutdown action is available at all times when steps to achieve a self-sustaining chain reaction are being intentionally taken or whenever a chain reaction might be initiated accidentally.
178	6	4.2.3.4. Normal heat removal	Principle: Heat transport systems are designed for highly reliable heat removal in normal operation. They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur.	204. The primary heat removal system is a reliable means of cooling the core in normal operation. It is also the preferred means of shutdown heat removal and for decay heat removal after an abnormal occurrence or in most accidents. There may be other systems, not necessarily safety related, but used in normal reactor operations, that can alternatively perform this important safety function of removal of residual heat. Their availability for use adds to defence in depth. For example, control rod drive pumps were used to maintain the reactor coolant inventory during the Browns Ferry fire in 1975.	The heat transport system fails to reliably remove heat in normal or accident conditions.	Heat transport systems are designed for highly reliable heat removal in normal operation. They would also provide means for the removal of heat from the reactor core during anticipated operational occurrences and during most types of accidents that might occur.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
179	6	4.2.3.5. Startup, shutdown, and low power operation	Principle: Components, structures, and systems used during startup, low power and shutdown operations are designed to maintain or restore the reactivity control, decay heat removal, and the integrity of the fission product barriers, so as to prevent the release of radioactive material resulting from accidents initiated during those operations.	206. During low power and shutdown operation, plant conditions can be different to those required for full power operation (see para. 62). During low power operation, reactivity coefficients may be different, and the plant may be operating far from the setpoints of certain automatic protective features. During shutdown, fuel handling may take place, the reactor coolant system and containment buildings may be open, and various systems and components may be out of service for maintenance or replacement. It is important for the reactor designer and the operating organization to consider these conditions so that sufficient redundancy, reliability and capacity in equipment, including instrumentation is provided in the design to assure adequate detection of, and protection against, conditions which could lead to exceeding specified limits. This includes considering loss of coolant inventory, decay heat removal and reactivity control.	Design and implementation of control and safety systems do not adequately take into account lower power and startup operation plant conditions.	Components, structures, and systems used during startup, low power and shutdown operations are designed to maintain or restore the reactivity control, decay heat removal, and the integrity of the fission product barriers, so as to prevent the release of radioactive material resulting from accidents initiated during those operations.
180	6	4.2.3.6. Emergency heat removal	Principle: Provision is made for alternative means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost.	208. Certain abnormal conditions could impair the capability to remove heat of all normal active in-plant systems. In some reactors, natural circulation would be adequate for decay heat removal in these circumstances, provided that the primary coolant boundary remains intact and some capability for heat removal is maintained on the secondary side. In other cases, for which severe core damage could possibly occur if no alternative heat removal path is provided, a capability for emergency heat removal is needed. This includes residual heat removal systems and emergency core cooling systems, and emergency feedwater systems to ensure the capability of heat removal on the secondary side. In the past, the unreliability of the shutdown heat removal function has been found to be a significant contributor to total risk for some nuclear plants. The need for highly reliable removal of shutdown heat has led in some cases to consideration of the use of special cooling system designs, such as dedicated and protected systems for decay heat removal and systems based on natural circulation or conduction. The atmosphere is sometimes considered as a possible ultimate heat sink.	Plant design and implementation does not adequately provide alternate means to restore and maintain fuel cooling under accident conditions.	Provision is made for alternative means to restore and maintain fuel cooling under accident conditions, even if normal heat removal fails or the integrity of the primary cooling system boundary is lost.

181	6	4.2.3.7. Reactor coolant system integrity	Principle: Codes and standards for nuclear vessels and piping are supplemented by additional measures to prevent conditions arising that could lead to a rupture of the primary coolant system boundary at any time during the operational lifetime of the plant.	210. The reactor coolant boundary is a critical system because its failure could lead to impairment of the ability to cool the fuel, and in extreme cases to loss of confinement of the radioactive fuel. This is particularly important for a pressurized reactor vessel, since catastrophic failure of this component would not be tolerable. 211. For all components forming part of the main coolant boundary, and especially for the reactor vessel, careful attention must be paid to design, materials, fabrication, installation, inspection and testing, with particular emphasis on use of established codes of practice and experienced suppliers, and detailed attention to the achievement of high quality. Analysis is carried out to demonstrate that the structures can withstand the stresses likely to be imposed under the more extreme expected loading conditions. 212. Multiple inspections are conducted during and after fabrication and installation of the primary system boundary. Ultrasonic, radiographic and surface methods are used. Hydraulic overpressure testing to pressures well above those expected in operation confirms the strength of the system before it is made radioactive. 213. Analyses of the strength of metallic parts of the primary system boundary are based on the assumption that small defects may have been introduced during manufacture and remained undetected in the inspection process owing to their small size. Such analyses show that design, operating restrictions and periodic inspections provide assurance, with an ample margin over the lifetime of the plant, that undetected cracks would not grow to a length or depth that would be critical under the maximum stresses to be encountered. Undue challenges to the integrity of the envelope of a pressurized reactor are prevented by ensuring adequate overpressure protection. For ferritic steel vessels, any combination of pressure and low temperature that might cause brittle failure (including combinations that might be encountered in design basis accidents) is prevented. Mechanisms of deterioration of the primary system boundary are taken into account in the design of the plant, including fatigue, corrosion, stress corrosion and embrittling effects of irradiation and of hydrogen. 214. The use of prestressed concrete pressure vessels is current practice for gas cooled reactor plants. Most statements made earlier generally apply to these as well, with differences only in detail, even though the structures are very different. An important additional requirement for such vessels is attention to the condition and loading of the prestressing tendons, and to the condition of the insulation, the liner, the liner cooling system, penetrations and similar features, as installed and subsequently in service. 215. During the lifetime of the plant, the continued fitness of the coolant boundary for service is verified by inspection, analysis and testing of exposed samples of archival vessel material, by monitoring for leaks using systems designed for this purpose, and by making any repairs or replacements that prove necessary and are feasible. Access for, ease of and frequency of inspection are taken into account in the design. 216. Ferritic steel reactor pressure vessels for some existing plants are subject to inspection and operating restrictions that would not be necessary if technological issues that are now understood had been well researched at the time of fabrication of the vessels. In future, welds are not to be made in regions of higher neutron flux levels, especially longitudinal welds at the vessel belt line. Steels for	Design, implementation and maintenance of the reactor coolant boundary is inadequate to prevent rupture.	Extra care should be taken for components that are critical to achieving safety

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				the vessels and welding consumables will have a very low content of elements that accelerate radiation induced deterioration, especially copper and phosphorus. Sensitive steels will not be used. Steels used will be readily weldable and, together with their weldments, will have high fracture toughness at all temperatures in the operating region. The vessels will have diameters large enough to ensure sufficient attenuation of the fast neutron flux between the core boundary and the vessels' inner surfaces.		
182	6	4.2.3.8. Confinement of radioactive material	Principle: The plant is designed to be capable of retaining the bulk of the radioactive material that might be released from fuel, for the entire range of accidents considered in the design.	218. A special system is required to retain radioactive material that might be released as a result of an accident, unless it has been shown that adequate protection against such a release has been secured by other means. No actual system could retain all the 57 radioactive material arising from a major accident, especially in view of the large inventory of radioactive noble gases. The special systems still have the function of preventing leakage of almost all the more significant radioactive materials. Such special systems providing a confinement function have common features. —A structure encloses the region into which radioactive material from fuel, consisting principally of fission products, could be released in the event of the loss of fuel integrity. —Confinement may be effected by making the structure so strong that when it is sealed it can withstand a high internal pressure. It is then called a containment structure. The containment structure usually has a subsystem that completes the sealing process on demand, and other subsystems protecting the structure (see the principle in Section 4.2.3.9). Together these constitute a containment system. —Confinement may be effected by equipping the structure with devices that permit pressure due to an accident to be relieved to the exterior while ensuring that the bulk of any radioactive material released from fuel is retained, e.g. on filters. —The structure maintains its integrity in both the short term and the long term under the pressure and temperature conditions that could prevail in design basis accidents. —Openings and penetrations, when they have been secured, and other singular points in the structure are designed to meet requirements similar to those for the structure itself so that they do not render it vulnerable as potential pathways for the release of radioactive material. —If analysis shows that residual reactor heat could lead to an increase of atmospheric temperature inside the containment and thereby generate a pressure threatening the integrity of the structure, provision is made for the removal of this heat. 219. It must be demonstrated that the confinement capability is such that the design basis targets for limiting the leakage of any radioactive material are met. Provision is therefore made for functional testing to ensure that design objectives are met. 220. Design measures are taken to prevent circumstances arising in which, in the event of an accident, radioactive materials could bypass the confinement and be released directly to the environment.	The plant design is not adequate to prevent the release of radioactive material that might be released from the fuel.	The plant is designed to be capable of retaining the bulk of the radioactive material that might be released from fuel, for the entire range of accidents considered in the design.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
183	6	4.2.3.9. Protection of confinement structure	Principle: If specific and inherent features of a nuclear power plant would not prevent detrimental effects on the confinement structure in a severe accident, special protection against the effects of such accidents is provided, to the extent needed to meet the general safety objective.	222. This principle particularly affects existing plants in which a confinement structure is used as a containment structure. A containment structure is designed to withstand the internal pressure that can be expected to result from the design basis accident for this structure, calculated using substantial safety factors. Calculations indicate that in extreme cases some severe accidents beyond the design basis could generate pressures higher than the design pressure for the containment structure. These higher values are in most cases less than those corresponding to the ultimate strength of the containment. 223. If severe accident sequences could lead to pressures causing stresses exceeding the estimated ultimate strength of the containment, that structure might fail. If it were to fail catastrophically early in the accident sequence, a significant release of radioactive material might occur, necessitating protective measures outside the plant. Such circumstances could produce an appreciable contribution to the calculated risk. 224. If this contribution to risk is so large as to conflict with the safety objectives, special measures to protect the containment structure are taken. Some measures that have been used or discussed in specific cases are hydrogen igniters, autocatalytic recombiners, filtered vent systems, area spray systems and fuel debris retainers (see Table II). 225. As noted in paras 25 and 27, a more systematic approach can be employed to improve the containment and/or confinement function for severe accidents in future nuclear power plants. 226. Similar considerations apply for confinement structures not designed for high internal pressures.	Confinement structure is not adequate to ensure that the general safety objective is satisfied during a severe accident.	If specific and inherent features of a nuclear power plant would not prevent detrimental effects on the confinement structure in a severe accident, special protection against the effects of such accidents is provided, to the extent needed to meet the general safety objective.
184	6	4.2.3.10. Monitoring of plant safety status	Principle: Parameters to be monitored in the control room are selected, and their displays are arranged, to ensure that operators have clear and unambiguous indications of the status of plant conditions important for safety, especially for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of defence in depth.	228. Continued knowledge and understanding of the status of the plant on the part of operating staff is a vital component of defence in depth. The control room is therefore provided with a display of the information on plant variables needed to ascertain the status in normal operation, to detect and diagnose off-normal conditions, and to observe the effect of corrective responses by control and safety systems. Information from both internally and externally initiated events is considered for control room display. Early warning of developing problems is provided, including loose part monitoring systems, monitoring of excessive and unusual vibration or noise, and systems to detect coolant leaks or unusual levels of radiation, temperatures or moisture. 229. The means of transmitting and displaying information include meters and status lights, parameter trend displays, prioritized alarms and various diagnostic aids as well as reliable personal communication between control room personnel and distant operating or maintenance staff. Care is taken by designers to ensure that the operators have the means of monitoring the most useful and important information, and to prevent distraction by more peripheral information. Experienced operating staff as well as human factor experts assist designers by identifying the most appropriate organization and presentation of these data.	The design and implementation of the human-machine interface is not adequate to ensure that operators have clear and unambiguous indication of status of plant conditions important to safety.	The human-machine interface should provide clear information to ascertain the status of the system and help diagnose off-normal conditions

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
185	6	4.2.3.11. Preservation of control capability	Principle: The control room is designed to remain habitable under normal operating conditions, anticipated abnormal occurrences and accidents considered in the design. Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which the main control room may be uninhabitable or damaged.	231. The environment in the control room is protected against abnormal conditions that might compromise the operators' effectiveness or jeopardize their health. These might be conditions arising in the plant or the result of some occurrence external to the plant. In the event that the environment of the control room is degraded for any reason, operators receive a clear warning. Suitable equipment for personal protection is provided. 232. Although unlikely, situations are conceivable in which the main control room could become uninhabitable or damaged to the extent that it is no longer usable. Alternative means are provided to ensure that safe plant conditions would be maintained if this happened. One or more supplementary locations are instrumented and equipped with the necessary controls so that the operators could take actions at these locations to ensure that the basic safety functions of reactor shutdown, residual heat removal and confinement of radioactive materials are achieved and maintained in the long term. Actions bringing about a change in system performance may sometimes need to be taken at remote locations, e.g. the local change of a valve setting. Where such control actions and monitoring are expected to occur at different points, communication between the points is reliable.	The design and implementation of the control room is inadequate to achieve habitability during accidents considered in the design. A remote control room is not provided, or is inadequate to provide remote monitoring and control required during an incident where the control room is uninhabitable.	The control room is designed to remain habitable under normal operating conditions, anticipated abnormal occurrences and accidents considered in the design. Independent monitoring and the essential capability for control needed to maintain ultimate cooling, shutdown and confinement are provided remote from the main control room for circumstances in which the main control room may be uninhabitable or damaged.
186	6	4.2.3.12. Station blackout	Principle: Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.	234. Electrical power is essential for nuclear power plant safety systems. Safety assessments show that the consequences of station blackout can be a dominant component of the total risk. The reliability of the electrical power supply is commensurate with the reliability demanded of the safety systems which it serves. Both normal and backup power supplies are designed to ensure high reliability. The reliability of backup electrical power supplies for safety systems is sometimes augmented by means of diverse power supplies, such as direct drive diesels, direct drive steam turbines and batteries for instruments and other DC components. 235. In particular, nuclear power plants are designed to withstand, without loss of safety function, a simultaneous loss of on-site and off-site AC electrical power (a station blackout) for a specified period of time. The period of time is a function of the plant design, the reliability of core cooling systems driven by other motive means, the ability to dissipate decay heat by other means, such as natural circulation and thermal conduction, and special provisions for restoring cooling or electrical power before damage occurs. 236. Additional electrical power generating sources (e.g. connection to a hydroelectric power station or installation of gas turbine generators) are used in some nuclear power plants to improve the response to station blackout.	Plant design is inadequate to prevent fuel damage in the event of simultaneous loss of on-site and off-site electrical power.	Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
187	6	4.2.3.13. Control of accidents within the design basis	Principle: Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents.	238. The plant operating staff are provided with appropriate safety equipment, instrumentation and operating procedures for response to and control of accidents within the design basis. Design is such that abnormal developments are first met automatically by the restoration of normal conditions by means of the feedback characteristics of neutronic and process controls. These are backed up by the normal capability for shutdown, continued cooling and protection against the release of radioactive materials. Further protection is available through automatic actuation of engineered safety systems. By means of such measures, any onset of abnormal behaviour would be dealt with automatically by appropriately designed systems for at least a predetermined period of time, during which the operating staff could assess systems, review possibilities and decide on a subsequent course of action for conditions not adequately responded to by the automatic functioning of plant systems. The design makes provision for diagnostic aids and symptom based emergency procedures for use in these circumstances. Typical decision intervals for operator action range from 10 to 30 minutes or longer depending on the situation. 239. The role of the operator in these circumstances is to ensure that all systems have responded correctly to the abnormal situation, to diagnose the abnormal event in a timely manner, to intervene if required and to restore critical safety functions. Instrumentation and information display systems support these roles, including safety parameter display systems and other sophisticated computer aids to help the operating staff trend and diagnose the evolution of accidents within the design basis.	The plant design is inadequate to control accidents within the design basis. The design of the information systems does not provide plant staff with adequate information for following and intervening in the course of an accident.	Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents.
188	6	4.2.3.14. New and spent fuel storage	Principle: Plant designs provide for the handling and storage of new and spent fuel in such a way as to ensure protection of workers and to prevent the release of radioactive material.	241. Facilities are required to handle and store new and spent fuel assemblies. The quantity of new and spent fuel to be stored varies with the design of the plant and the individual refuelling requirements. The storage facilities keep the new and spent fuel in a safe and subcritical array under all anticipated storage conditions. The facilities and fuel racks take into account external loads and forces (e.g. in an earthquake). Since the spent fuel contains a significant inventory of fission products, shielding from radiation and a safe means of loading the assemblies into shipping casks are provided. The integrity of spent fuel cladding is preserved by redundant and reliable means of removing decay heat. Provision is also made for inspecting new and spent fuel, for testing, handling and storing defective fuel, and for retrieving fuel for remedial action, e.g. for shipping it off-site for post-irradiation examination. Monitoring for radioactive releases, ensuring subcriticality, providing physical protection and continued cooling of the spent fuel are important elements in operating such facilities	The plant design for handling and storage of new fuel is inadequate to protect workers or prevent the release of radioactive materials.	Plant designs provide for the handling and storage of new and spent fuel in such a way as to ensure protection of workers and to prevent the release of radioactive material.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
189	6	4.2.3.15. Plant physical protection	Principle: The design and operation of a nuclear power plant provide adequate measures to protect the plant from damage and to prevent the unauthorized release of radioactive material arising from unauthorized acts by individuals or groups, including trespass, unauthorized diversion or removal of nuclear materials, and sabotage of the plant.	243. Protection of the plant and equipment from unauthorized acts is already ensured by design features provided for other reasons, such as locating redundant safety equipment in different areas of the plant and providing for an emergency control room. Additional physical protection is provided through a designed combination of security hardware and devices, security guards, and appropriate layout and design of the facility for access control. Physical protection issues are considered early in the planning stages of a nuclear power plant. In addition, a physical protection audit is carried out at the design stage on the basis of potential threats. An active protection programme is in effect from receipt of the first batch of fuel to the final stages of decommissioning. Emergency physical protection procedures are available to handle effectively any possible threats. 244. Physical protection measures are co-ordinated with nuclear safety programmes to ensure that physical protection is not jeopardizing nuclear safety. For example, physical protection measures will not jeopardize nuclear safety under emergency conditions.	The design and operation of the plant is inadequate to provide protection from unauthorized acts.	Design and operation of the system should provide protection from unauthorized acts by individuals or groups that may impact safety
190	6	4.3.1. Safety evaluation of design	Principle: Construction of a nuclear power plant is begun only after the operating organization and the regulatory organization have satisfied themselves by appropriate assessments that the main safety issues have been satisfactorily resolved and that the remainder are amenable to solution before operations are scheduled to begin.	247. The options available to the designers for modifying plant safety features become restricted as fabrication and construction proceed. For this reason it is necessary to co-ordinate safety evaluation with manufacturing and construction to ensure that important safety options are not foreclosed and that licensing decisions are timely. 248. At approximately the stage when preliminary design has been completed a safety analysis is performed. This overall analysis is reviewed with the regulatory authorities to ensure that regulatory requirements have been met or will be met, and the plant will be safe for operation. This determination may be subject to outstanding issues expected to be resolved during construction and before operation starts. Additional check points are established as required during construction so that satisfactory final design, installation and verification of the adequacy of safety related equipment can be reviewed.	Plant construction begins before agreement is achieved with the regulator on the assessment of plant safety.	Safety of the design of the system should be assessed before the system is constructed
192	6	4.4.1. Verification of design and construction	Principle: The commissioning programme is established and followed to demonstrate that the entire plant, especially items important to safety and radiation protection, has been constructed and functions according to the design intent, and to ensure that weaknesses are detected and corrected.	256. To ensure that the design intent has been met, the commissioning programme includes checks of safety equipment and its functional characteristics, and of provisions for radiation protection. Testing is progressive; less onerous conditions are achieved first and hold points are used to ensure that adequate test results are obtained before proceeding to the next stage. The commissioning programme and its results are subject to surveillance and review by the regulatory authorities. Some phases of commissioning take place during construction. Elements of systems are tested; as complete systems are finished, they are also tested. Variations from the design intent that are found in these checks are assessed, corrected and referred to the operating organization so that any effect on plant operation can be taken into account. Where complete tests of components and systems under realistic conditions cannot be made, tests are performed in combination under conditions as close as possible to realistic. 257. Commissioning continues through fuel loading, criticality and power ascension. Commissioning results are subject to close review by the regulatory authorities. They are also used by designers to improve future plant designs	The commissioning programme is inadequate to demonstrate that the plant is compliant with its safety requirements.	Commissioning of the system should demonstrate that the plant is compliant with its safety requirements

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
215	7	Level 1	1) Prevention of abnormal operation and failures	- the clear definition of normal and abnormal operating conditions; - adequate margins in the design of systems and plant components, including robustness and resistance to accident conditions, in particular aimed at minimizing the need to take measures at Level 2 and Level 3; - adequate time for operators to respond to events and appropriate human-machine interfaces, including operator aids, to reduce the burden on the operators; - careful selection of materials and use of qualified fabrication processes and proven technology together with extensive testing; - comprehensive training of appropriately selected operating personnel whose behaviour is consistent with a sound safety culture; - adequate operating instructions and reliable monitoring of plant status and operating conditions; - recording, evaluation and utilization of operating experience; - comprehensive preventive maintenance prioritized in accordance with the safety significance and reliability requirements of systems.	The design and implementation of the plant is inadequate to prevent abnormal operations and failures in compliance with reliability requirements.	- the clear definition of normal and abnormal operating conditions; - adequate margins in the design of systems and plant components, including robustness and resistance to accident conditions, in particular aimed at minimizing the need to take measures at Level 2 and Level 3; - adequate time for operators to respond to events and appropriate human-machine interfaces, including operator aids, to reduce the burden on the operators; - careful selection of materials and use of qualified fabrication processes and proven technology together with extensive testing; - comprehensive training of appropriately selected operating personnel whose behaviour is consistent with a sound safety culture; - adequate operating instructions and reliable monitoring of plant status and operating conditions; - recording, evaluation and utilization of operating experience; - comprehensive preventive maintenance prioritized in accordance with the safety significance and reliability requirements of systems.
216	7	Level 2	2) Control of abnormal operation and detection of failures	- incorporates inherent plant features - core stability and thermal inertia, and - systems to control abnormal operation (anticipated operational occurrences), - with account taken of phenomena capable of causing further deterioration in the plant status. - The systems to mitigate the consequences of such operating occurrences are designed according to specific criteria (such as redundancy, layout and qualification). - Diagnostic tools and equipment such as automatic control systems can be provided to actuate corrective actions before reactor protection limits are reached - Ongoing surveillance of quality and compliance with the design assumptions by means of in-service inspection and periodic testing of systems and plant components	Plant design and implementation is inadequate to control abnormal operations or to detect equipment failures.	- comprehensive hazard analysis - complete set of features to mitigate all identified causes of hazards - ongoing surveillance to detect non-compliances with design assumptions and program to implement fixes in a timely manner

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
217	7	Level 3	3) Control of accidents within the design basis	- Engineered safety features and protection systems are provided to prevent evolution towards severe accidents and also to confine radioactive materials within the containment system - Design and operating procedures are aimed at maintaining the effectiveness of the barriers, especially the containment, in the event of such a postulated accident - High reliability of engineered safety systems by following design principles: - redundancy; - prevention of common mode failure due to internal or external hazards, by physical or spatial separation and structural protection; - prevention of common mode failure due to design, manufacturing, construction, commissioning, maintenance or other human intervention, by diversity or functional redundancy; - automation to reduce vulnerability to human failure, at least in the initial phase of an incident or an accident; - testability to provide clear evidence of system availability and performance; -qualification of systems, components and structures for specific environmental conditions that may result from an accident or an external hazard.	Plant design is inadequate to prevent accidents from evolving to severe accidents.	- comprehensive hazard analysis - complete set of engineered safety features - achievement of high reliability engineered safety systems by applying design principles such as: - redundancy; - prevention of common mode failure due to internal or external hazards, by physical or spatial separation and structural protection; - prevention of common mode failure due to design, manufacturing, construction, commissioning, maintenance or other human intervention, by diversity or functional redundancy; - automation to reduce vulnerability to human failure, at least in the initial phase of an incident or an accident; - testability to provide clear evidence of system availability and performance; -qualification of systems, components and structures for specific environmental conditions that may result from an accident or an external hazard.
218	7	Level 4	4) Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	- Consideration is given to severe plant conditions that were not explicitly addressed in the original design (Levels 1 to 3) of currently operating plants owing to their very low probabilities - may be caused by multiple failures - may be caused by an extremely unlikely event - Measures for accident management are also aimed at controlling the course of severe accidents and mitigating their consequences - to monitor the main characteristics of plant status; - to control core subcriticality; - to restore heat removal from the core and maintain long term core cooling; -to protect the integrity of the containment by ensuring heat removal and preventing dangerous loads on the containment in the event of severe core damage or further accident progression; - regaining control of the plant if possible and, if degradation cannot be stopped, delaying further plant deterioration and implementing on-site and off-site emergency response.	Plant design is inadequate to mitigate the consequences of a severe accident.	- accident management measures in place to: - to monitor the main characteristics of plant status; - to control core subcriticality; - to restore heat removal from the core and maintain long term core cooling; -to protect the integrity of the containment by ensuring heat removal and preventing dangerous loads on the containment in the event of severe core damage or further accident progression; - regaining control of the plant if possible and, if degradation cannot be stopped, delaying further plant deterioration and implementing on-site and off-site emergency response.

DESIGN AND CONSTRUCTION PHASE

Technology

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
1	1	Requirement 4: Fundamental safety functions	Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.	4.1. A systematic approach shall be taken to identifying those items important to safety that are necessary to fulfil the fundamental safety functions and to identifying the inherent features that are contributing to fulfilling, or that are affecting, the fundamental safety functions for all plant states. 4.2. Means of monitoring the status of the plant shall be provided for ensuring that the required safety functions are fulfilled.	Lack of Compliance with Fundamental Safety Requirements	Systematic approach to design plant to satisfy control, cool and contain. Design means to monitor compliance with control, cool and contain.
2	1	Requirement 5: Radiation protection in design	The design of a nuclear power plant shall be such as to ensure that radiation doses to workers at the plant and to members of the public do not exceed the dose limits, that they are kept as low as reasonably achievable in operational states for the entire lifetime of the plant, and that they remain below acceptable limits and as low as reasonably achievable in, and following, accident conditions.	4.3. The design shall be such as to ensure that plant states that could lead to high radiation doses or to a large radioactive release have been ‘practically eliminated', and that there would be no, or only minor, potential radiological consequences for plant states with a significant likelihood of occurrence. 4.4. Acceptable limits for purposes of radiation protection associated with the relevant categories of plant states shall be established, consistent with the regulatory requirements.	Safety Risk Not ALARA	Design ensures that the risk of radiological accidents is as low as reasonably practical.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
3	1	Requirement 6: Design for a nuclear power plant	The design for a nuclear power plant shall ensure that the plant and items important to safety have the appropriate characteristics to ensure that safety functions can be performed with the necessary reliability, that the plant can be operated safely within the operational limits and conditions for the full duration of its design life and can be safely decommissioned, and that impacts on the environment are minimized.	4.5. The design for a nuclear power plant shall be such as to ensure that the safety requirements of the operating organization, the requirements of the regulatory body and the requirements of relevant legislation, as well as applicable national and international codes and standards, are all met, and that due account is taken of human capabilities and limitations and of factors that could influence human performance. Adequate information on the design shall be provided for plant modifications to be made. Recommended practices shall be provided for incorporation into the administrative and operational procedures for the plant (i.e. the operational limits and conditions). 4.6. The design shall take due account of relevant available experience that has been gained in the design, construction and operation of other nuclear power plants, and of the results of relevant research programmes. 4.7. The design shall take due account of the results of deterministic safety analyses and probabilistic safety analyses, to ensure that due consideration is given to the prevention of accidents and to mitigation of the consequences of any accidents that do occur. 4.8. The design shall be such as to ensure that the generation of radioactive waste and discharges are kept to the minimum practicable in terms of both activity and volume, by means of appropriate design measures and operational and decommissioning practices.	Lack of Compliance with Fundamental Safety Requirements	Design satisfies all regulatory requirements and applicable national and international standards. Design takes into account applicable operating experience. The design shall take into account measures that prevent accidents and mitigate the consequences of accidents that do occur.

4	1	Requirement 7: Application of defence in depth	The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable.	4.9. The defence in depth concept shall be applied to provide several levels of defence that are aimed at preventing consequences of accidents that could lead to harmful effects on people and the environment, and ensuring that appropriate measures are taken for the protection of people and the environment and for the mitigation of consequences in the event that prevention fails. 4.10. The design shall take due account of the fact that the existence of multiple levels of defence is not a basis for continued operation in the absence of one level of defence. All levels of defence in depth shall be kept available at all times and any relaxations shall be justified for specific modes of operation. 4.11. The design: (a) Shall provide for multiple physical barriers to the release of radioactive material to the environment; (b) Shall be conservative, and the construction shall be of high quality, so as to provide assurance that failures and deviations from normal operation are minimized, that accidents are prevented as far as is practicable and that a small deviation in a plant parameter does not lead to a cliff edge effect;9 (c) Shall provide for the control of plant behaviour by means of inherent and engineered features, such that failures and deviations from normal operation requiring actuation of safety systems are minimized or excluded by design, to the extent possible; (d) Shall provide for supplementing the control of the plant by means of automatic actuation of safety systems, such that failures and deviations from normal operation that exceed the capability of control systems can be controlled with a high level of confidence, and the need for operator actions in the early phase of these failures or deviations from normal operation is minimized; (e) Shall provide for systems, structures and components and procedures to control the course of and, as far as practicable, to limit the consequences of failures and deviations from normal operation that exceed the capability of safety systems; (f) Shall provide multiple means for ensuring that each of the fundamental safety functions is performed, thereby ensuring the effectiveness of the barriers and mitigating the consequences of any failure or deviation from normal operation. 4.12. To ensure that the concept of defence in depth is maintained, the design shall prevent, as far as is practicable: (a) Challenges to the integrity of physical barriers; (b) Failure of one or more barriers; (c) Failure of a barrier as a consequence of the failure of another barrier; (d) The possibility of harmful consequences of errors in operation and maintenance. 4.13. The design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the nuclear power plant.	Lack of Compliance with Fundamental Safety Requirements	Design utilizes defense-in-depth principle to achieve control, cool and contain with a high degree of confidence.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
5	1	Requirement 8: Interfaces of safety with security and safeguards	Safety measures, nuclear security measures and arrangements for the State system of accounting for, and control of, nuclear material for a nuclear power plant shall be designed and implemented in an integrated manner so that they do not compromise one another.	4.14. Items important to safety for a nuclear power plant shall preferably be of a design that has previously been proven in equivalent applications, and if not, shall be items of high quality and of a technology that has been qualified and tested. 4.15. National and international codes and standards that are used as design rules for items important to safety shall be identified and evaluated to determine their applicability, adequacy and sufficiency, and shall be supplemented or modified as necessary to ensure that the quality of the design is commensurate with the associated safety function. 4.16. Where an unproven design or feature is introduced or where there is a departure from an established engineering practice, safety shall be demonstrated by means of appropriate supporting research programmes, performance tests with specific acceptance criteria or the examination of operating experience from other relevant applications. The new design or feature or new practice shall also be adequately tested to the extent practicable before being brought into service, and shall be monitored in service to verify that the behaviour of the plant is as expected.	Lack of Compliance with Fundamental Safety Requirements	Use of proven designs, compliant with applicable national and international standards with adequate demonstration of achievement of safety requirements.
6	1	Requirement 12: Features to facilitate radioactive waste management and decommissioning	Special consideration shall be given at the design stage of a nuclear power plant to the incorporation of features to facilitate radioactive waste management and the future decommissioning and dismantling of the plant.	4.20. In particular, the design shall take due account of: (a) The choice of materials, so that amounts of radioactive waste will be minimized to the extent practicable and decontamination will be facilitated; (b) The access capabilities and the means of handling that might be necessary; (c) The facilities necessary for the management (i.e. segregation, characterization, classification, pretreatment, treatment and conditioning) and storage of radioactive waste generated in operation, and provision for managing the radioactive waste that will be generated in the decommissioning of the plant.	Inadequate Radioactive Waste Management	Design takes into account choice of materials so that the amount of radioactive waster generated is minimized to the extent practicable Design includes facilities to manage radioactive waste
7	1	Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant	Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.	5.63. To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design.	Safety Risk Not ALARA	Consider opportunities for increasing safety utilizing capabilities of multi-unit stations in the design

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
8	1	Requirement 34: Systems containing fissile material or radioactive material	All systems in a nuclear power plant that could contain fissile material or radioactive material shall be so designed as: to prevent the occurrence of events that could lead to an uncontrolled radioactive release to the environment; to prevent accidental criticality and overheating; to ensure that radioactive releases are kept below authorized limits on discharges in normal operation and below acceptable limits in accident conditions, and are kept as low as reasonably achievable; and to facilitate mitigation of radiological consequences of accidents.	None	Safety Risk Not ALARA	Design systems containing radioactive material to prevent occurrence of events that could lead to uncontrolled release to the environment, prevent overheating, to contain releases of radioactive material and to facilitate mitigation of radiological consequence in accident conditions.
9	1	Requirement 35: Nuclear power plants used for cogeneration of heat and power, heat generation or desalination	Nuclear power plants coupled with heat utilization units (such as for district heating) and/or water desalination units shall be designed to prevent processes that transport radionuclides from the nuclear plant to the desalination unit or the district heating unit under conditions of operational states and in accident conditions .	None	Safety Risk Not ALARA	Design to prevent processes that transport radioactive material external to the plant.
10	1	Requirement 36: Escape routes from the plant	A nuclear power plant shall be provided with a sufficient number of escape routes, clearly and durably marked, with reliable emergency lighting, ventilation and other services essential to the safe use of these escape routes.	5.64. Escape routes from the nuclear power plant shall meet the relevant national and international requirements for radiation zoning and fire protection, and the relevant national requirements for industrial safety and plant security. 5.65. At least one escape route shall be available from workplaces and other occupied areas following an internal event or an external event or following combinations of events considered in the design.	Inadequate Emergency Management	Design sufficient escape routes meeting national and international standards.
11	1	Requirement 37: Communication systems at the plant	Effective means of communication shall be provided throughout the nuclear power plant to facilitate safe operation in all modes of normal operation and to be available for use following all postulated initiating events and in accident conditions.	5.66. Suitable alarm systems and means of communication shall be provided so that all persons present at the nuclear power plant and on the site can be given warnings and instructions, in operational states and in accident conditions. 5.67. Suitable and diverse means of communication necessary for safety within the nuclear power plant and in the immediate vicinity, and for communication with relevant off-site agencies, shall be provided.	Inadequate Emergency Management	Design suitable communications systems to be able to communicate to personnel during operations and during an emergency with sufficient redundancy and diversity.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
12	1	Requirement 38: Control of access to the plant	The nuclear power plant shall be isolated from its surroundings with a suitable layout of the various structural elements so that access to it can be controlled.	5.68. Provision shall be made in the design of the buildings and the layout of the site for the control of access to the nuclear power plant by operating personnel and/or for equipment, including emergency response personnel and vehicles, with particular consideration given to guarding against the unauthorized entry of persons and goods to the plant.	Inadequate Emergency Management	Design access controls to the plant.
13	1	Requirement 39: Prevention of unauthorized access to, or interference with, items important to safety	Unauthorized access to, or interference with, items important to safety, including computer hardware and software, shall be prevented.	None	Inadequate Emergency Management	Design system important to safety to prevent unauthorized access.
14	1	Requirement 40: Prevention of harmful interactions of systems important to safety	The potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and effects of any harmful interactions shall be prevented.	5.69. In the analysis of the potential for harmful interactions of systems important to safety, due account shall be taken of physical interconnections and of the possible effects of one system's operation, maloperation or malfunction on local environmental conditions of other essential systems, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended. 5.70. If two fluid systems important to safety are interconnected and are operating at different pressures, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to prevent the design pressure of the system operating at the lower pressure from being exceeded.	Lack of Compliance with Fundamental Safety Requirements	The design takes into account interactions between systems to ensure that failures of systems providing redundant or diverse safety functionality do not have common cause failures.
15	1	Requirement 41: Interactions between the electrical power grid and the plant	The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.	None	Lack of Compliance with Fundamental Safety Requirements	The safety functions of systems important to safety are designed to not be impacted by disturbances of the power grid.

OPERATIONS AND MAINTENANCE PHASE

Business Process

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
40	1	Requirement 29: Calibration, testing, maintenance, repair, replacement, inspection and monitoring of items important to safety	Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis.	5.45. The plant layout shall be such that activities for calibration, testing, maintenance, repair or replacement, inspection and monitoring are facilitated and can be performed to relevant national and international codes and standards. Such activities shall be commensurate with the importance of the safety functions to be performed, and shall be performed without undue exposure of workers. 5.46. Where items important to safety are planned to be calibrated, tested or maintained during power operation, the respective systems shall be designed for performing such tasks with no significant reduction in the reliability of performance of the safety functions. Provisions for calibration, testing, maintenance, repair, replacement or inspection of items important to safety during shutdown shall be included in the design so that such tasks can be performed with no significant reduction in the reliability of performance of the safety functions. 5.47. If an item important to safety cannot be designed to be capable of being tested, inspected or monitored to the extent desirable, a robust technical justification shall be provided that incorporates the following approach: (a) Other proven alternative and/or indirect methods such as surveillance testing of reference items or use of verified and validated calculational methods shall be specified. (b) Conservative safety margins shall be applied or other appropriate precautions shall be taken to compensate for possible unanticipated failures.	Ageing and wearout mechanisms cause equipment performance to degrade over time causing a noncompliance with safety requirements including reliability and dependability requirements	Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements Design margins established to account for unanticipated failures. Robust technical justification for the inspection and maintenance program.
42	2	Requirement 10: Control of plant configuration	The operating organization shall establish and implement a system for plant configuration management to ensure consistency between design requirements, physical configuration and plant documentation.	4.38. Controls on plant configuration shall ensure that changes to the plant and its safety related systems are properly identified, screened, designed, evaluated, implemented and recorded. Proper controls shall be implemented to handle changes in plant configuration that result: from maintenance work, testing, repair, operational limits and conditions, and plant refurbishment; and from modifications due to ageing of components, obsolescence of technology, operating experience, technical developments and results of safety research.	Noncompliance with safety requirements resulting from changes to plant configuration due to maintenance work, refurbishment work or operation outside of safe operating envelope	Establishment of controls on plant configuration that ensures changes to plant configuration are consistent with the established safe operating envelope
42	2	Requirement 10: Control of plant configuration	The operating organization shall establish and implement a system for plant configuration management to ensure consistency between design requirements, physical configuration and plant documentation.	4.38. Controls on plant configuration shall ensure that changes to the plant and its safety related systems are properly identified, screened, designed, evaluated, implemented and recorded. Proper controls shall be implemented to handle changes in plant configuration that result: from maintenance work, testing, repair, operational limits and conditions, and plant refurbishment; and from modifications due to ageing of components, obsolescence of technology, operating experience, technical developments and results of safety research.	Noncompliance with safety requirements resulting from changes to plant configuration due to maintenance work, refurbishment work or operation outside of safe operating envelope	Establishment of controls on plant configuration that ensures changes to plant configuration are consistent with the established safe operating envelope

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
45	2	Requirement 15: Records and reports	The operating organization shall establish and maintain a system for the control of records and reports.	4.52. The operating organization shall identify the types of record and report, as specified by the regulatory body, that are relevant for the safe operation of the plant. Records of operation, including maintenance and surveillance, shall be kept available from initial testing during the startup of each plant system important to safety, including relevant off-site tests. The records of operation shall be retained in proper archives for the periods required by the regulatory body. All records shall be kept readable, complete, identifiable and easily retrievable [3]. Retention times for records and reports shall be commensurate with their level of importance for the purposes of operation and plant licensing and for future decommissioning.	Inadequate maintenance and surveillance to maintain equipment performance consistent with safety requirements	Establish a system of controls for records and reports related to safety related maintenance and surveillance
46	2	Requirement 16: Programme for long term operation	Where applicable, the operating organization shall establish and implement a comprehensive programme for ensuring the long term safe operation of the plant beyond a time-frame established in the licence conditions, design limits, safety standards and/or regulations.	4.53. The justification for long term operation shall be prepared on the basis of the results of a safety assessment, with due consideration of the ageing of structures, systems and components. The justification for long term operation shall utilize the results of periodic safety review and shall be submitted to the regulatory body, as required, for approval on the basis of an analysis of the ageing management programme, to ensure the safety of the plant throughout its extended operating lifetime. 4.54. The comprehensive programme for long term operation shall address: (a) Preconditions (including the current licensing basis, safety upgrading and verification, and operational programmes); (b) Setting the scope for all structures, systems and components important to safety; (c) Categorization of structures, systems and components with regard to degradation and ageing processes; (d) Revalidation of safety analyses made on the basis of time limited assumptions; (e) Review of ageing management programmes in accordance with national regulations; (f) The implementation programme for long term operation.	Equipment ageing changes equipment performance such that safety requirements are not satisfied	Establish an ageing management program to maintain the performance of structures, systems and components that have an impact on safety

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
48	2	Requirement 18: Emergency preparedness	The operating organization shall prepare an emergency plan for preparedness for, and response to, a nuclear or radiological emergency.	5.2. Emergency arrangements shall cover the capability of maintaining protection and safety in the event of an accident; mitigating the consequences of accidents if they do occur; protection of site personnel and the public; protection of the environment; coordinating response organizations, as appropriate; and communicating with the public in a timely manner [1, 6]. Emergency arrangements shall include arrangements for: the prompt declaration of an emergency; timely notification and alerting of response personnel; assessment of the progress of the emergency, its consequences and any measures that need to be taken on the site; and the necessary provision of information to the authorities. Appropriate arrangements shall be established from the time that nuclear fuel is first brought to the site, and the emergency plan and all emergency arrangements shall be completed before the commencement of fuel loading. 5.3. The operating organization shall develop an emergency plan and shall establish the necessary organizational structure, with assigned responsibilities for managing an emergency, and shall contribute to the development of off-site emergency procedures. 5.4. The emergency plan shall cover all activities under the responsibility of the operating organization and it shall be adhered to in the event of an emergency. The emergency plan shall include arrangements for an emergency involving a combination of non-radiological hazards and radiological hazards, such as a fire in conjunction with significant levels of radiation or contamination, or toxic or asphyxiating gases in conjunction with radiation or contamination. Account shall be taken in the emergency plan of the specific site conditions. Preparation of the emergency plan shall be coordinated with those bodies having responsibilities in an emergency, including public authorities and private enterprises, as relevant, and the plan shall be submitted to the regulatory body as required. The plan shall be subject to review and updating in the light of experience gained. 5.5. A training programme for emergencies shall be established and implemented to ensure that plant staff and, as required, staff from other participating organizations possess the essential knowledge, skills and attitudes required for the accomplishment of non-routine tasks under stressful emergency conditions. 5.6. The emergency plan shall be tested and validated in exercises before the commencement of fuel loading. Emergency preparedness training, exercises and drills shall be planned and conducted at suitable intervals, to evaluate the preparedness of plant staff and staff from external response organizations to perform their tasks, and to evaluate their cooperation in coping with an emergency and in improving the efficiency of the response [1, 6]. 5.7. Facilities, instruments, tools, equipment, documentation and communication systems to be used in an emergency, including those needed for off-site communication and for the accident management programme, shall be kept available. They shall be maintained in good operational condition in such a manner that they are unlikely to be affected by, or made unavailable by, accidents. The operating organization shall ensure that relevant information on safety parameters is available in the emergency response facilities and locations, as appropriate, and that communication between the control rooms and these facilities and locations is effective in the event of an accident [2]. These capabilities shall be tested periodically.	Inadequate protection of the public in the event of an accident.	Establishment of a comprehensive emergency plan for responding to a nuclear or radiological emergency Establishment of the necessary organizational structures for managing and emergency Establishment of a training program so that personnel have the necessary competencies to execute the emergency plan in response to an accident Establishment of, and maintenance of the facilities and equipment necessary to execute the emergency plan in response to an accident

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
49	2	Requirement 19: Accident management programme	The operating organization shall establish, and shall periodically review and as necessary revise, an accident management programme.	5.8. An accident management programme shall be established that covers the preparatory measures, procedures and guidelines, and equipment that are necessary for preventing the progression of accidents, including accidents more severe than design basis accidents, and for mitigating their consequences if they do occur. The accident management programme shall be documented and shall be periodically reviewed and as necessary revised. 5.8A. For a multi-unit nuclear power plant site, concurrent accidents affecting all units shall be considered in the accident management programme. Trained and experienced personnel, equipment, supplies and external support shall be made available for coping with concurrent accidents. Potential interactions between units shall be considered in the accident management programme. 5.8B. The accident management programme shall include instructions for the utilization of available equipment — safety related equipment as far as possible, but also items not important to safety (e.g. conventional equipment). 5.8C. The accident management programme shall include contingency measures, such as an alternative supply of cooling water and an alternative supply of electrical power, to mitigate the consequences of accidents, including any necessary equipment. This equipment shall be located and maintained so as to be functional and readily accessible when needed. 5.8D. The accident management programme shall include the technical and administrative measures necessary to mitigate the consequences of an accident. 5.8E. The accident management programme shall include training necessary for implementation of the programme. 5.8F. In developing the accident management programme and its procedures, the possibility of regional infrastructure being degraded and of adverse working conditions (e.g. elevated radiation levels, elevated temperatures, lack of lighting, limited access to the plant from off the site) for operators, as well as the possibility of operating conditions for equipment being degraded, shall be taken into account so as to ensure that actions expected for accident management will be feasible and will be able to be taken in a timely and reliable manner. 5.9. Arrangements for accident management shall provide the operating staff with appropriate competence, systems and technical support. These arrangements and relevant guidance shall be available before the commencement of fuel loading, shall be validated and shall then be periodically tested as far as practicable in exercises and used in training and drills [1, 6]. In addition, arrangements shall be made, as part of the accident management programme and the emergency plan, to expand the emergency arrangements, where necessary, to include the responsibility for long term actions.	Failure to prevent the progression of an accident	Establishment of an accident management program that covers preparatory measures, procedures, guidelines and equipment necessary for preventing the progression of accidents and mitigating the consequences of accidents. Competent personnel and supporting equipment necessary to deal with accidents including concurrent accidents. Contingency measures including alternative supply of cooling water and alternate supply of electrical power. Accident management program that takes into account the possibility of regional infrastructure being degraded and of adverse working conditions, as well as the possibilty that operating conditions for equipment will be degraded.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
50	2	Requirement 2: Management system	The operating organization shall establish, implement, assess and continually improve an integrated management system.	3.4. The operating organization shall ensure through the establishment and use of a management system that the plant is operated in a safe manner and within the limits and conditions that are specified in the safety assessment and established in the authorization. 3.5. The management system shall integrate all the elements of management so that processes and activities that may affect safety are established and conducted coherently with other requirements, including requirements in respect of leadership, protection of health, human performance, protection of the environment, security and quality, and so that safety is not compromised by other requirements or demands. 3.6. The management system of the operating organization shall provide for arrangements to ensure safety in activities performed by external support organizations. Responsibility for activities performed by external support organizations, and for their overall control and supervision, rests with the operating organization. The operating organization shall establish a system for the supervision of work performed by support organizations. It shall be the responsibility of the operating organization to ensure that the personnel of external support organizations who perform activities on structures, systems or components important to safety or activities affecting safety are qualified to perform their assigned tasks. The overall contracted activity shall be clearly specified in writing and shall be approved by the operating organization prior to its commencement. The operating organization shall ensure long term access to knowledge of the plant design and manufacturing and construction throughout the lifetime of the plant. 3.7. The operational safety of a plant is subject to oversight by a regulatory body independent of the operating organization. The operating organization, in accordance with the regulatory requirements, shall submit or make available to the regulatory body all necessary documents and information. The operating organization shall develop and implement a procedure for reporting events to the regulatory body in accordance with the established criteria and the State's regulations. The operating organization shall provide the regulatory body with all necessary assistance to enable it to perform its duties, including enabling unhindered access to the plant and providing documentation.	Operation of the plant outside its safe operating envelope Unsatisfied safety requirement	Establishment and use of a management system that ensures that the plant is operated in a safe manner and within the safe operating envelope

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
51	2	Requirement 20: Radiation protection	The operating organization shall establish and implement a radiation protection programme.	5.10. The operating organization shall ensure that the radiation protection programme is in compliance with the requirements of Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards (No. GSR Part 3) [8]. The operating organization shall verify, by means of surveillance, inspections and audits, that the radiation protection programme is being properly implemented and that its objectives are being met. The radiation protection programme shall be reviewed on a regular basis and shall be updated if necessary. 5.11. The radiation protection programme shall ensure that for all operational states, doses due to exposure to ionizing radiation at the plant or doses due to any planned radioactive releases (discharges) from the plant are kept below authorized limits and are as low as reasonably achievable. 5.12. The radiation protection programme in the operating organization shall have sufficient independence and resources to be able to enforce and to advise on radiation protection regulations, standards and procedures, and on safe working practices. 5.13. All plant personnel shall understand and acknowledge their individual responsibility for putting into practice the measures for controlling exposures that are specified in the radiation protection programme. Consequently, particular emphasis shall be given to the training of all site personnel so that they are aware of radiological hazards and of the necessary protective measures. 5.14. All site personnel, including contractors, who are working in a controlled area or who are regularly present in a supervised area shall have their occupational exposures assessed in accordance with the requirements of GSR Part 3 [8]. Dose records shall be kept and shall be made available to personnel on demand and to the regulatory body. 5.15. The radiation protection programme shall include the workers' health surveillance of site personnel who may be occupationally exposed to radiation for ascertaining their physical fitness and for giving advice in cases of accidental overexposure. This workers' health surveillance shall consist of a preliminary medical examination followed by periodic checkups. 5.16. The radiation protection programme shall ensure control over radiation dose rates for exposures due to activities in areas where there is radiation arising from or passing through structures, systems and components, such as in inspection, maintenance and fuel handling. It also addresses plant chemistry activities as well as exposures due to radioactivity of substances in the fuel coolant (liquid or gas) and associated fluids. The programme shall make arrangements to maintain these doses as low as reasonably achievable.	Non compliance with the safety related governance programmes established by the organization	Establishing a program of surveillances, inpsections and audits to verify compliance with safety related governance programs Establish training programs to ensure that all personnel understand their responsibilities with respect to safety

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
52	2	Requirement 21: Management of radioactive waste	The operating organization shall establish and implement a programme for the management of radioactive waste.	5.17. Adequate operating practices shall be implemented to ensure that the generation of radioactive waste is kept to the minimum practicable in terms of both activity and volume. 5.18. The operating organization shall establish and implement a programme for the management of radioactive waste. The programme for the management of radioactive waste shall include the characterization, classification, processing (i.e. pretreatment, treatment and conditioning), transport, storage and disposal of radioactive waste, as well as regular updating of the inventory of radioactive waste. Processing and storage of radioactive waste shall be strictly controlled in a manner consistent with the requirements for the predisposal management of radioactive waste [4]. Records shall be maintained for waste generation and waste classification, as well as for the processing, storage and disposal of waste. 5.19. The operating organization shall establish and implement procedures consistent with international standards, national regulations and licence conditions for the monitoring and control of discharges of radioactive effluents. These procedures shall be made available to the regulatory body if required. The volume and activity of radioactive discharges to the environment shall be reported periodically to the regulatory body. 5.20. The operating organization shall ensure that a programme is established and implemented for monitoring the environment in the vicinity of the plant site, to assess radiological consequences of any radioactive releases to the environment. Results from this monitoring shall be made available to the public and in particular to the public living in the vicinity of the plant site.	Exposure to radiation from radioactive waste or effluents.	Establish operating practices that keep generation of radioactive waste to a minimum Establish and implement a radioactive waste management program to manage the processing, transport, storage and disposal of radioactive waste

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
53	2	Requirement 22: Fire safety	The operating organization shall make arrangements for ensuring fire safety.	5.21. The arrangements for ensuring fire safety made by the operating organization shall cover the following: adequate management for fire safety; preventing fires from starting; detecting and extinguishing quickly any fires that do start; preventing the spread of those fires that have not been extinguished; and providing protection from fire for structures, systems and components that are necessary to shut down the plant safely. Such arrangements shall include, but are not limited to: (a) Application of the principle of defence in depth; (b) Control of combustible materials and ignition sources, in particular during outages; (c) Inspection, maintenance and testing of fire protection measures; (d) Establishment of a manual firefighting capability; (e) Assignment of responsibilities and training and exercising of plant personnel; (f) Assessment of the impact of plant modifications on fire safety measures. 5.22. A comprehensive fire hazard analysis shall be developed for the plant and shall be periodically reviewed and, if necessary, updated. 5.23. In the arrangements for firefighting, special attention shall be paid to cases for which there is a risk of release of radioactive material in a fire. Appropriate measures shall be established for the radiation protection of firefighting personnel and the management of releases to the environment. 5.24. The operating organization shall be responsible for ensuring that appropriate procedures, equipment and staff are in place for effectively coordinating and cooperating with all firefighting services involved. Periodic joint fire drills and exercises shall be conducted to assess the effectiveness of the fire response capability. 5.25. Fire protection systems and firefighting systems shall be designed to ensure that damage to, or inadvertent operation of, these systems does not significantly impair the capabilities of the structures, systems and components necessary for safe shutdown.	Fire	Establish and implement a fire safety program Establish fire hazard analysis as part of the overall plant hazard analysis Establish procedures, equipment and staffing to coordinate with firefighting services
54	2	Requirement 23: Non-radiation-related safety	The operating organization shall establish and implement a programme to ensure that safety related risks associated with non-radiation-related hazards to personnel involved in activities at the plant are kept as low as reasonably achievable.	5.26. The non-radiation-related safety programme shall include arrangements for the planning, implementation, monitoring and review of the relevant preventive and protective measures, and it shall be integrated with the nuclear and radiation safety programme. All personnel, suppliers, contractors and visitors (where appropriate) shall be trained and shall possess the necessary knowledge of the non-radiation-related safety programme and its interface with the nuclear and radiation safety programme, and shall comply with its safety rules and practices. The operating organization shall provide support, guidance and assistance for plant personnel in the area of non-radiation-related hazards.	Non-radiation-related hazard	Establish a non-radiation-related safety program and integrate it into the radiation-related safety program

55	2	Requirement 26: Operating procedures	Operating procedures shall be developed that apply comprehensively (for the reactor and its associated facilities) for normal operation, anticipated operational occurrences and accident conditions, in accordance with the policy of the operating organization and the requirements of the regulatory body.	6.1. The commissioning programme for the plant shall cover the full range of plant conditions required in the design and the safety case. The results shall be used to demonstrate that the behaviour of the plant as built is in compliance with the design assumptions and the licence conditions. Special attention shall be paid to ensuring that no commissioning tests are performed that might place the plant in an unanalysed condition. Commissioning stages, test objectives and acceptance criteria shall be specified in such a way that the programme is auditable. 6.2. The commissioning programme shall provide the operating organization and the regulatory body with the means of identifying the hold points in the commissioning process at which approval may be required prior to continuing to the next stage. 6.3. The commissioning programme shall be divided into stages. A review of the test results for each stage shall be completed before commissioning is continued to the next stage. On the basis of the review, a judgement shall be made on whether the commissioning programme can proceed to the next stage. Judgements shall also be made on the basis of the review on whether the succeeding stages will be modified as a consequence of the test results, or because some tests in the stage had not been undertaken, or some tests had been undertaken but had not been completed. The results for some stages may be subject to approval by the regulatory body before commissioning can proceed to the next stage. 6.4. The commissioning programme shall include all the tests necessary to demonstrate that the plant as built and as installed meets the requirements of the safety analysis report and satisfies the design intent and, consequently, that the plant can be safely operated in accordance with the operational limits and conditions. 6.5. Operating and maintenance procedures shall be validated to the extent practicable as part of the commissioning programme, with the participation of future operating personnel. 6.6. Suitably qualified operations personnel shall be directly involved in the commissioning process. Operating personnel and plant technical staff shall be involved in the commissioning process to the extent necessary to ensure proper preparation for the operational phase. 6.7. The commissioning programme shall be sufficiently comprehensive as to provide reference data to characterize structures, systems and components. Such reference data shall be retained as they are important for ensuring the safety of the plant and for subsequent safety reviews. 6.8. All the functions of the operating organization shall be performed at the appropriate stages during commissioning. These functions shall include discharging responsibilities for management, training of personnel, the radiation protection programme, waste management, managements of records, fire safety, physical protection and the emergency plan. 6.9. Operating procedures and test procedures shall be verified to ensure their technical accuracy and shall be validated to ensure their usability with the installed equipment and control systems. Verification and validation of procedures shall be performed to confirm their applicability and quality, and to the extent possible shall be performed prior to fuel handling operations on the site. This process shall continue during the commissioning phase. Verification and validation shall also be	Operating the plant outside its safe operating envelope	Establish and implement a commissioning program that demonstrates that the plant as built is compliant with all design assumptions and licensing conditions Establish operating and maintenance procedures necessary to keep the plant operating within its safe operating envelope and validate the procedures as part of the commissioning program

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				carried out for procedures for overall operation. 6.10. From the commencement of commissioning, reviewed and approved arrangements for work control, modification control and plant configuration control shall be in place to meet the conditions of the commissioning tests. 6.11. Initial fuel loading shall not be authorized until all relevant pre-operational tests have been performed and the results have been accepted by the operating organization and the regulatory body. Reactor criticality and initial power increase shall not be authorized until all necessary tests have been performed and the results have been accepted by the operating organization and the regulatory body, as appropriate. The tests of the commissioning programme shall be successfully completed as a necessary condition for authorization, as appropriate, for normal operation of the plant to be commenced. 6.12. The operating organization shall ensure that the interfaces and the communication lines between different groups (i.e. groups for design, groups for construction, contractors, groups for commissioning and groups for operations) shall be clearly specified and controlled. 6.13. Authorities and responsibilities shall be clearly specified and shall be delegated to the individuals and groups performing the commissioning activities. The operating organization shall be responsible for ensuring that construction activities are of appropriate quality and that completion data on commissioning activities and comprehensive baseline data, documentation or information are provided. The operating organization shall also be responsible for ensuring that the equipment supplied is manufactured under a quality assurance programme that includes inspection for proper fabrication, cleanliness, calibration and verification of operability. 6.14. During construction and commissioning, the plant shall be monitored, preserved and maintained so as to protect plant equipment, to support the testing stage and to maintain consistency with the safety analysis report. 6.15. During construction and commissioning, a comparison shall be carried out between the as built plant and its design parameters. A comprehensive process shall be established to address non-conformances in design, manufacturing, construction and operation. Resolutions to correct differences from the initial design and non-conformances shall be documented.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
56	2	Requirement 27: Operation control rooms and control equipment	The operating organization shall ensure that the operation control rooms and control equipment are maintained in a suitable condition.	7.7. The habitability and good condition of control rooms shall be maintained. Where the design of the plant foresees additional or local control rooms that are dedicated to the control of processes that could affect plant conditions, clear communication lines shall be developed for ensuring an adequate transfer of information to the operators in the main control room. 7.8. The supplementary control room (sometimes known as a remote shutdown panel) and all other safety related operational panels outside the control room shall be kept operable and free from obstructions, as well as from non-essential material that would prevent their immediate operation. The operating organization shall periodically confirm that the supplementary control room and all other safety related operational panels are in the proper state of operational readiness, including proper documentation, communications, alarm systems and habitability. 7.9. The alarms in the main control room shall be managed as an important feature in operating a plant safely. The plant information system shall be such that off-normal conditions are easily recognizable by the operators. Control room alarms shall be clearly prioritized. The number of alarms, including alarm messages from process computers, shall be minimized for any analysed operational state, outage or accident condition of the plant. The operating organization shall establish procedures for operators to manage the response to alarms.	Control rooms become inhabitable	Establish a supplementary control room Establish training programs on the use of the supplementary control room Establish a maintenance program to keep the supplementary control room functional
57	2	Requirement 28: Material conditions and housekeeping	The operating organization shall develop and implement programmes to maintain a high standard of material conditions, housekeeping and cleanliness in all working areas.	7.10. Administrative controls shall be established to ensure that operational premises and equipment are maintained, well lit and accessible, and that temporary storage is controlled and limited. Equipment that is degraded (owing to leaks, corrosion spots, loose parts or damaged thermal insulation, for example) shall be identified and reported and deficiencies shall be corrected in a timely manner. 7.11. An exclusion programme for foreign objects shall be implemented and monitored, and suitable arrangements shall be made for locking, tagging or otherwise securing isolation points for systems or components to ensure safety. 7.12. The operating organization shall be responsible for ensuring that the identification and labelling of safety equipment and safety related equipment, rooms, piping and instruments are accurate, legible and well maintained, and that they do not introduce any degradation.	Equipment and staff performance does not satisfy safety requirements	Establish a hosekeeping program to ensure that operational premises and equipment are maintained, well lit and accessible

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
58	2	Requirement 29: Chemistry programme	The operating organization shall establish and implement a chemistry programme to provide the necessary support for chemistry and radiochemistry.	7.13. The chemistry programme shall be developed prior to normal operation and shall be in place during the commissioning programme. The chemistry programme shall provide the necessary information and assistance for chemistry and radiochemistry for ensuring safe operation, long term integrity of structures, systems and components, and minimization of radiation levels. 7.14. Chemistry surveillance shall be conducted at the plant to verify the effectiveness of chemistry control in plant systems and to verify that structures, systems and components important to safety are operated within the specified chemical limit values. 7.15. The chemistry programme shall include chemistry monitoring and data acquisition systems. These systems, together with laboratory analyses, shall provide accurate measuring and recording of chemistry data and shall provide alarms for relevant chemistry parameters. Records shall be kept available and shall be easily retrievable. 7.16. Laboratory monitoring shall involve the sampling and analysis of plant systems for specific chemical parameters, concentrations of dissolved and suspended impurities, and radionuclide concentrations. 7.17. The use of chemicals in the plant, including chemicals brought in by contractors, shall be kept under close control. The appropriate control measures shall be put in place to ensure that the use of chemical substances and reagents does not adversely affect equipment or lead to its degradation.	Degradation of equipment due to poor chemistry	Establish and implement a chemistry program

59	2	Requirement 30: Core management and fuel handling	The operating organization shall be responsible and shall make arrangements for all activities associated with core management and with on-site fuel handling.	7.18. Provision shall be made to ensure that only fuel that has been appropriately manufactured is loaded into the core. In addition, the fuel design criteria and fuel enrichment shall be in accordance with design specifications and shall be subject to approval by the regulatory body as required. The same requirements shall be applied before the introduction of fuel of a new design or of a modified design into the core. 7.19. The operating organization shall be responsible for the development of the specifications and procedures for the procurement, verification, receipt, accounting and control, loading, utilization, relocation, unloading and testing of fuel and core components. A fuelling programme shall be established in accordance with the design assumptions and details shall be submitted to the regulatory body if required. Following refuelling, it shall be confirmed by means of calculations and measurements that the performance of the core meets the safety criteria. It shall also be confirmed that all core alterations comply with approved configurations. 7.20. The operating organization shall be responsible for establishing a safe reactivity management programme under a strong management system for quality. Decisions on, and the planning, evaluation, conduct and control of, all operations or modifications involving the fuel that are liable to affect reactivity control shall be undertaken by using approved procedures and respecting predefined operational limits for the core. 7.21. A comprehensive core monitoring programme shall be established to ensure that core parameters are monitored, analysed for trends and evaluated to detect abnormal behaviour; to ensure that actual core performance is consistent with core design requirements; and to ensure that the values of key operating parameters are recorded and retained in a logical, consistent and retrievable manner. 7.22. Reactivity manipulations shall be made in a deliberate and carefully controlled manner to ensure that the reactor is maintained within prescribed operational limits and conditions and that the desired response is achieved. 7.23. The operating procedures for reactor startup, power operation, shutdown and refuelling shall include the precautions and limitations necessary to maintain fuel integrity and to comply with the operational limits and conditions throughout the lifetime of the fuel. 7.24. Radiochemistry data that are indicative of fuel cladding integrity shall be systematically monitored and analysed for trends so as to be able to monitor whether fuel cladding integrity is maintained under all operating conditions. 7.25. Appropriate methods shall be established to identify any anomalous changes in the activity of coolant and to perform data analysis for fuel defects to determine their nature and severity, their location, their probable root causes and the necessary corrective actions.	Nuclear fuel does not meet its safety requirements Plant is not operated within its safe operating envelope with respect to nuclear reactivity	Establish and implement a safe reactivity management program

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				7.26. For fuel and core components, handling procedures shall be developed to ensure the controlled movement of unirradiated and irradiated fuel, proper storage on the site and preparation for transport from the site. The plans for storage of unirradiated and irradiated fuel shall be submitted to the regulatory body for approval, if so required. 7.27. The packaging, carriage and transport of unirradiated and irradiated fuel shall be carried out in accordance with appropriate national regulations for domestic transport and, in the event of international transport, with IAEA Safety Standards Series No. SSR-6, Regulations for the Safe Transport of Radioactive Material [9]. 7.28. Before any fuel handling takes place, the operating organization shall ensure that an authorized, trained and qualified person is present, who shall be responsible for control and handling of the fuel on the site in accordance with written procedures. Access to fuel storage areas shall be limited to authorized personnel. 7.29. Detailed auditable accounts shall be maintained as required for the storage, irradiation and movement of all fissile material, including unirradiated and irradiated fuel, for at least as long as the regulatory body requires in regulations.		

60	2	Requirement 31: Maintenance, testing, surveillance and inspection programmes	The operating organization shall ensure that effective programmes for maintenance, testing, surveillance and inspection are established and implemented.	8.1. Maintenance, testing, surveillance and inspection programmes shall be established that include predictive, preventive and corrective maintenance activities. These maintenance activities shall be conducted to maintain availability during the service life of structures, systems and components by controlling degradation and preventing failures. In the event that failures do occur, maintenance activities shall be conducted to restore the capability of failed structures, systems and components to function within acceptance criteria. 8.2. The operating organization shall establish surveillance programmes for ensuring compliance with established operational limits and conditions and for detecting and correcting any abnormal condition before it can give rise to significant consequences for safety. 8.3. The operating organization shall develop procedures for all maintenance, testing, surveillance and inspection tasks. These procedures shall be prepared, reviewed, modified when required, validated, approved and distributed in accordance with procedures established under the management system. 8.4. Data on maintenance, testing, surveillance and inspection shall be recorded, stored and analysed for the purpose of confirming that the operating performance is in accordance with the design intent and with requirements for the reliability and availability of equipment. 8.5. The frequency of maintenance, testing, surveillance and inspection of individual structures, systems and components shall be determined on the basis of: (a) The importance to safety of the structures, systems and components, with insights from probabilistic safety assessment taken into account; (b) Their reliability in, and availability for, operation; (c) Their assessed potential for degradation in operation and their ageing characteristics; (d) Operating experience; (e) Recommendations of vendors. 8.6. A comprehensive and structured approach to identifying failure scenarios shall be taken to ensure the proper management of maintenance activities, using methods of probabilistic safety analysis as appropriate. 8.7. New approaches that could result in significant changes to current strategies for maintenance, testing, surveillance and inspection shall be taken only after careful consideration of the implications for safety and after appropriate authorization, as required. 8.8. A comprehensive work planning and control system shall be implemented to ensure that work for purposes of maintenance, testing, surveillance and inspection is properly authorized, is carried out safely and is documented in accordance with established procedures. 8.9. An adequate work control system shall be established for the protection and safety of personnel and for the protection of equipment during maintenance, testing, surveillance and inspection. Pertinent information shall be transferred at shift turnovers and at pre-job and post-job briefings on maintenance, testing, surveillance and inspection. 8.10. The work control system shall ensure that plant equipment is released from service for maintenance, testing, surveillance or inspection only with the authorization of designated operations department staff and in compliance with	Equipment fails to perform consistent with its safety requirements	Establish a maintenance program for all equipment that is related to performing safety functions in the plant

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				the operational limits and conditions. The work control system shall also ensure that permission to return equipment to service following maintenance, testing, surveillance and inspection is given by the operating personnel. Such permission shall be given only after the completion of a documented check that the new plant configuration is within the established operational limits and conditions and, where appropriate, after functional tests have been performed. 8.11. Coordination shall be maintained between different maintenance groups (e.g. maintenance groups for mechanical, electrical, instrumentation and control, and civil equipment). Coordination shall also be maintained between maintenance groups, and operations groups and support groups (e.g. groups for fire protection, radiation protection, physical protection and non-radiation-related safety). The operating organization shall make arrangements with the external grid operator to ensure that appropriate procedures are applied in maintaining the connections of the plant to the external grid. 8.12. A management system for managing and correcting deficiencies shall be established and shall be used to ensure that operating personnel are not overly burdened. This system shall also ensure that safety at the plant is not compromised by the cumulative effects of these deficiencies. 8.13. The operating organization shall ensure that maintenance work during power operation is carried out with adequate defence in depth. Probabilistic safety assessment shall be used, as appropriate, to demonstrate that the risks are not significantly increased. 8.14. Corrective maintenance of structures, systems and components shall be performed as promptly as practicable and in compliance with operational limits and conditions. Priorities shall be established, with account taken first of the relative importance to safety of the defective structures, systems and components. 8.14A. The operating organization shall establish maintenance programmes for non-permanent equipment to be used for accidents more severe than design basis accidents [2], in order to maintain high reliability of this equipment. The operating organization shall carry out periodic training and exercises in handling the equipment and connecting it to the nuclear power plant. 8.15. The operating organization shall establish suitable arrangements to procure, receive, control, store and issue materials (including supplies), spare parts and components. 8.16. The operating organization shall be responsible for using these arrangements for the procurement of materials (including supplies), spare parts and components and for ensuring that their characteristics are consistent with applicable safety standards and with the plant design. 8.17. The operating organization shall ensure that storage conditions are adequate and that materials (including supplies), spare parts and components are available and are in proper condition for use.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
61	2	Requirement 32: Outage management	The operating organization shall establish and implement arrangements to ensure the effective performance, planning and control of work activities during outages.	8.18. Outage planning shall be a continuing, improving process involving past, present, next scheduled and future outages. Reference points shall be determined and shall be used to track pre-outage work. 8.19. In the processes for planning and performing outage activities, priority shall be given to safety related considerations. Special attention shall be given to maintaining the plant configuration in accordance with the operational limits and conditions. 8.20. The operating organization shall be responsible for issuing programmes and procedures for outage management and for the provision of adequate resources for ensuring safety during shutdown operations. 8.21. The tasks, authorities and responsibilities of the groups and persons involved in preparing, conducting or assessing outage schedules and activities shall be set out in writing and shall be followed by all the plant staff and contractor staff who are involved. 8.22. The interfaces between the group responsible for outages and other groups, including groups on the site and off the site, shall be clearly defined. Operating personnel shall be kept informed of current activities for maintenance, modification and testing. 8.23. Optimization of radiation protection, optimizing of non-radiation-related safety, waste reduction and control of chemical hazards shall be essential elements of outage programmes and planning, and this shall be clearly communicated to relevant plant staff and contractors. 8.24. A comprehensive review shall be performed after each outage to draw lessons to be learned.	Safety related design modifications and maintenance is not performed in a timely manner	Establish and implement a program for the planning and execution of online and offline maintenance and design modification activities

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
62	2	Requirement 33: Preparation for decommissioning	The operating organization shall prepare a decommissioning plan and shall maintain it throughout the lifetime of the plant, unless otherwise approved by the regulatory body, to demonstrate that decommissioning can be accomplished safely and in such a way as to meet the specified end state.	9.1. The decommissioning plan shall be updated in accordance with changes in regulatory requirements, modifications to the plant, advances in technology, changes in the need for decommissioning activities and changes in national policies [5]. 9.2. A human resource programme shall be developed for ensuring that sufficient motivated and qualified personnel are available for the safe operation of the plant up to final shutdown, for conducting activities in a safe manner during the preparatory period for decommissioning and for safely carrying out the decommissioning of the plant. 9.3. In the preparatory period for decommissioning, a high level of operational safety shall be maintained until the nuclear fuel has been removed from the plant. 9.4. For a multiple unit plant, appropriate measures shall be put in place to ensure that common systems and common equipment remain fully available to support the safe operation of all the generating units. 9.5. The operating organization shall be aware, over the operating lifetime of the plant, of the needs in relation to future decommissioning. Experience and knowledge with regard to contaminated or irradiated structures, systems and components gained in modification and maintenance activities at the plant shall be recorded and retained to facilitate the planning of decommissioning. Complete and reviewed information shall be compiled to be transferred to the organization responsible for managing the decommissioning phase. 9.6. The implications for safety of the activities in the transitional phase prior to the commencement of decommissioning shall be assessed and shall be managed so as to avoid undue hazards and to ensure safety.	Safety requirements are not satisfied during the decommissioning of the plant	Establish a decommissioning plan

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
63	3	Requirement 10: Management of processes and activities	Processes and activities shall be developed and shall be effectively managed to achieve the organization's goals without compromising safety.	4.28. Each process shall be developed and shall be managed to ensure that requirements are met without compromising safety. Processes shall be documented and the necessary supporting documentation shall be maintained. It shall be ensured that process documentation is consistent with any existing documents of the organization. Records to demonstrate that the results of the respective process have been achieved shall be specified in the process documentation. 4.29. The sequencing of a process and the interactions between processes shall be specified so that safety is not compromised. Effective interaction between interfacing processes shall be ensured. Particular consideration shall be given to interactions between processes within the organization, and to interactions between processes conducted by the organization and processes conducted by external service providers. 4.30. New processes or modifications to existing processes shall be designed, verified, approved and applied so that safety is not compromised. Processes, including any subsequent modifications to them, shall be aligned with the goals, strategies, plans and objectives of the organization. 4.31. Any activities for inspection, testing, and verification and validation, their acceptance criteria and the responsibilities for carrying out such activities shall be specified. It shall be specified when and at what stages independent inspection, testing, and verification and validation are required to be conducted. 4.32. Each process or activity that could have implications for safety shall be carried out under controlled conditions, by means of following readily understood, approved and current procedures, instructions and drawings. These procedures, instructions and drawings shall be validated before their first use and shall be periodically reviewed to ensure their adequacy and effectiveness. Individuals carrying out such activities shall be involved in the validation and the periodic review of such procedures, instructions and drawings.	Safety related performance of equipment or personnel is impacted negatively by non-safety related activities	Establish non-safety related programs taking into account any potential impacts to safety related equipment or activities

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
64	3	Requirement 11: Management of the supply chain	The organization shall put in place arrangements with vendors, contractors and suppliers for specifying, monitoring and managing the supply to it of items, products and services that may influence safety.	4.33. The organization shall retain responsibility for safety when contracting out any processes and when receiving any item, product or service in the supply chain 4.34. The organization shall have a clear understanding and knowledge of the product or service being supplied. The organization shall itself retain the competence to specify the scope and standard of a required product or service, and subsequently to assess whether the product or service supplied meets the applicable safety requirements. 4.35. The management system shall include arrangements for qualification, selection, evaluation, procurement, and oversight of the supply chain. 4.36. The organization shall make arrangements for ensuring that suppliers of items, products and services important to safety adhere to safety requirements and meet the organization's expectations of safe conduct in their delivery.	Products or services from vendors, contractors or suppliers do not satisfy safety requirements	Establish and implement a program for the qualification, selection, evaluation, procurement and oversight of the suppy chain
69	3	Requirement 5: Interaction with interested parties	Senior management shall ensure that appropriate interaction with interested parties takes place.	4.6. Senior management shall identify interested parties for their organization and shall define an appropriate strategy for interaction with them. 4.7. Senior management shall ensure that the processes and plans resulting from the strategy for interaction with interested parties include: (a) Appropriate means of communicating routinely and effectively with and informing interested parties with regard to radiation risks associated with the operation of facilities and the conduct of activities; (b) Appropriate means of timely and effective communication with interested parties in circumstances that have changed or that were unanticipated; (c) Appropriate means of dissemination to interested parties of necessary information relevant to safety; (d) Appropriate means of considering in decision making processes the concerns and expectations of interested parties in relation to safety.	Lack of actions necessary to maintain safety when changes occur in the basis of the safety case for the plant	Establishment of a program for identification and effective communication with parties interested in the safety of the plant
71	3	Requirement 7: Application of the graded approach to the management system	The management system shall be developed and applied using a graded approach.	4.15. The criteria used to grade the development and application of the management system shall be documented in the management system. The following shall be taken into account: (a) The safety significance and complexity of the organization, operation of the facility or conduct of the activity; (b) The hazards and the magnitude of the potential impacts (risks) associated with the safety, health, environmental, security, quality and economic elements of each facility or activity [16, 24–26]; (c) The possible consequences for safety if a failure or an unanticipated event occurs or if an activity is inadequately planned or improperly carried out.	The safety significance of changes to the plant and its processes and organization are not taken into account	Establishment of a safety management system that takes into account the safety significance of changes

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
108	4	Requirement 9: System for protective actions to reduce existing or unregulated radiation risks	The government shall establish an effective system for protective actions to reduce undue radiation risks associated with unregulated sources (of natural or artificial origin) and contamination from past activities or events, consistent with the principles of justification and optimization.	2.25. Radiation risks may arise in situations other than in facilities and activities that are in compliance with regulatory control. In such situations, if the radiation risks are relatively high, consideration shall be given to whether protective actions can reasonably be taken to reduce radiation exposures and to remediate adverse conditions [1]. Where unacceptable radiation risks arise as a consequence of an accident, a discontinued practice, or inadequate control over a radioactive source or a natural source, the government shall designate the organizations to be responsible for making the necessary arrangements for the protection of workers, the public and the environment [6]. The organization taking the protective action shall have access to the resources necessary to fulfil its function. 2.26. The regulatory body shall provide any necessary inputs for the protective action, including advising the government or exercising regulatory control over protective actions. It shall establish the regulatory requirements and criteria for protective actions in cooperation with the other authorities involved, and in consultation with interested parties, as appropriate. 2.27. International assistance may have to be requested if there are insufficient resources available nationally to take protective actions.		
113	4	Requirement 14: International obligations and arrangements for international cooperation and assistance	The government shall fulfil its respective international obligations, participate in the relevant international arrangements, including international peer reviews, and promote international cooperation and assistance to enhance safety globally.	3.2. The features of the global safety regime include: (a) International conventions that establish common obligations and mechanisms for ensuring protection and safety; (b) Codes of conduct that promote the adoption of good practices in the relevant facilities and activities; (c) Internationally agreed IAEA safety standards that promote the development and application of internationally harmonized safety requirements, guides and practices; (d) International peer reviews of the regulatory control and safety of facilities and activities, and mutual learning by participating States; (e) Regular multilateral and bilateral cooperation between the relevant national and international organizations to enhance safety by means of harmonized approaches as well as to increase the quality and effectiveness of safety reviews and inspections, by means of sharing of knowledge and feedback of experience. 3.2A. The government shall ensure that bilateral and multilateral arrangements are in place for benefiting from international cooperation and, as appropriate, from the provision of assistance in connection with a nuclear or radiological emergency [5, 8].		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
114	4	Requirement 15: Sharing of operating experience and regulatory experience	The regulatory body shall make arrangements for analysis to be carried out to identify lessons to be learned from operating experience and regulatory experience, including experience in other States, and for the dissemination of the lessons learned and for their use by authorized parties, the regulatory body and other relevant authorities.	3.3. The reporting of operating experience and regulatory experience has led to significant corrective actions in relation to equipment, human performance and the management system for safety, as well as changes to regulatory requirements and modifications to regulatory practices. 3.4. The regulatory body shall establish and maintain a means for receiving information from other States, regulatory bodies of other States, international organizations and authorized parties, as well as a means for making available to others lessons learned from operating experience and regulatory experience. The regulatory body shall require appropriate corrective actions to be carried out to prevent the recurrence of safety significant events. This process involves acquisition of the necessary information and its analysis to facilitate the effective utilization of international networks for learning from operating experience and regulatory experience. 3.5. To enhance the safety of facilities and activities globally, feedback shall be provided on measures that have been taken in response to information received via national and international knowledge and reporting networks. Such measures could comprise promulgation of new regulatory requirements or making safety enhancing modifications to operating practices or to equipment in authorized facilities and activities. Such feedback provided in response to information received via international networks also covers descriptions of good practices that have been adopted to reduce radiation risks. 3.5A. Relevant information and lessons learned from operating experience and regulatory experience shall be reported in a timely manner to international knowledge and reporting networks.		
120	4	Requirement 21: Liaison between the regulatory body and authorized parties	The regulatory body shall establish formal and informal mechanisms of communication with authorized parties on all safety related issues, conducting a professional and constructive liaison.	4.23. As its primary purpose, the regulatory body shall carry out oversight of facilities and activities. The regulatory body, while maintaining its independence, shall liaise with authorized parties to achieve their common objectives in ensuring safety. Meetings shall be held as necessary to fully understand and discuss the arguments of each party on safety related issues. 4.24. The regulatory body shall foster mutual understanding and respect on the part of authorized parties through frank, open and yet formal relationships, providing constructive liaison on safety related issues and in-depth technical dialogue between experts. 4.25. The decisions of the regulatory body shall be justified as appropriate, and the basis for the decisions shall be explained.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
124	4	Requirement 25: Review and assessment of information relevant to safety	The regulatory body shall review and assess relevant information — whether submitted by the authorized party or the vendor, compiled by the regulatory body, or obtained from elsewhere — to determine whether facilities and activities comply with regulatory requirements and the conditions specified in the authorization. This review and assessment of information shall be performed prior to authorization and again over the lifetime of the facility or the duration of the activity, as specified in regulations promulgated by the regulatory body or in the authorization.			

125	4	Requirement 26: Graded approach to review and assessment of a facility or an activity	Review and assessment of a facility or an activity shall be commensurate with the radiation risks associated with the facility or activity, in accordance with a graded approach.	4.39A. The regulatory body shall ensure, adopting a graded approach, that authorized parties routinely evaluate operating experience and periodically perform comprehensive safety reviews of facilities, such as periodic safety reviews for nuclear power plants [11]. These comprehensive safety reviews are submitted to the regulatory body for assessment or are made available to the regulatory body. The regulatory body shall ensure that any reasonably practicable safety improvements identified in the reviews are implemented in a timely manner. 4.40. The regulatory body shall review and assess the particular facility or activity in accordance with the stage in the regulatory process (initial review, subsequent reviews, reviews of changes to safety related aspects of the facility or activity, reviews of operating experience, or reviews of long term operation, life extension, decommissioning or release from regulatory control). The depth and scope of the review and assessment of the facility or activity by the regulatory body shall be commensurate with the radiation risks associated with the facility or activity, in accordance with a graded approach. 4.41. Technical and other documents submitted by the applicant shall be reviewed and assessed by the regulatory body to determine whether the facility or activity complies with the relevant objectives, principles and associated criteria for safety. 4.42. In performing its review and assessment of the facility or activity, the regulatory body shall acquire an understanding of the design of the facility or equipment, the concepts on which the safety of the design is based and the operating principles proposed by the applicant, to satisfy itself that, among other factors: (a) The available information demonstrates the safety of the facility or the proposed activity and the optimization of protection [1, 6]. (b) The information provided in the applicant's submissions is accurate and is sufficient to permit confirmation of compliance with regulatory requirements. (c) Operational and technical provisions, and in particular any novel provision, have been proved or qualified by experience or testing, or both, and will enable the required level of safety to be achieved. 4.43. The regulatory body shall assess the radiation risks associated with normal operation, anticipated operational occurrences and accidents, including possible events with a very low probability of occurrence, prior to operation of the facility or conduct of the activity, and periodically throughout the lifetime of the facility or the duration of the activity, to determine whether radiation risks are as low as reasonably achievable. 4.44. Any proposed modification that might significantly affect the safety of a facility or activity shall be subject to a review and assessment by the regulatory body. 4.45. In the process of its review and assessment of the facility or activity, the regulatory body shall take into account such considerations and factors as: (1) The regulatory requirements; (2) The nature and categorization of the associated hazards; (3) The site conditions and the operating environment;

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				(4) The basic design of the facility or the conduct of the activity as relevant to safety; (5) The records provided by the authorized party or its suppliers; (6) Best practices; (7) The applicable management system; (8) The competence and skills necessary for operating the facility or conducting the activity; (9) Arrangements for protection (of workers, the public, patients and the environment) [6]; (10) Arrangements for preparedness for, and response to, emergencies; (11) Arrangements for nuclear security; (12) The system of accounting for, and control of, nuclear material; (13) The relevance of applying the concept of defence in depth to take into account inherent uncertainties (e.g. in the long term for the disposal of radioactive waste); (14) Arrangements for the management of radioactive sources, radioactive waste and spent fuel; (15) Relevant research and development plans or programmes relating to the demonstration of safety; (16) Feedback of operating experience, nationally and internationally, and especially of relevant operating experience from similar facilities and activities; (17) Information compiled in regulatory inspections; (18) Information from research findings; (19) Arrangements for the termination of operations. 4.46. For an integrated safety assessment, the regulatory body shall first organize the results obtained in a systematic manner. It shall then identify trends and conclusions drawn from inspections, from reviews and assessments for operating facilities, and from the conduct of activities where relevant. Feedback information shall be provided to the authorized party. This integrated safety assessment shall be repeated periodically, with account taken of the radiation risks associated with the facility or activity, in accordance with a graded approach. 4.47. Risks that are not related to radiation may arise in the operation of facilities or the conduct of activities, and these risks shall also be taken into account in the decision making process of the regulatory body. 4.48. The regulatory body shall record the results and decisions deriving from reviews and assessments, and shall take appropriate action (including enforcement action) as necessary. The results of reviews and assessments shall be used as feedback information for the regulatory process.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
126	4	Requirement 27: Inspection of facilities and activities	The regulatory body shall carry out inspections of facilities and activities to verify that the authorized party is in compliance with the regulatory requirements and with the conditions specified in the authorization.			
127	4	Requirement 28: Types of inspection of facilities and activities	Inspections of facilities and activities shall include programmed inspections and reactive inspections, both announced and unannounced.			

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
128	4	Requirement 29: Graded approach to inspections of facilities and activities	Inspections of facilities and activities shall be commensurate with the radiation risks associated with the facility or activity, in accordance with a graded approach.	4.49. Regulatory inspection cannot diminish the prime responsibility for safety of the authorized party, and cannot substitute for the control, supervision and verification activities conducted under the responsibility of the authorized party. 4.50. The regulatory body shall develop and implement a programme of inspection of facilities and activities, to confirm compliance with regulatory requirements and with any conditions specified in the authorization. In this programme, it shall specify the types of regulatory inspection (including scheduled inspections and unannounced inspections), and shall stipulate the frequency of inspections and the areas and programmes to be inspected, in accordance with a graded approach. 4.51. The regulatory body shall record the results of inspections and shall take appropriate action (including enforcement actions as necessary). Results of inspections shall be used as feedback information for the regulatory process and shall be provided to the authorized party. 4.52. Regulatory inspections shall cover all areas of responsibility of the regulatory body, and the regulatory body shall have the authority to carry out independent inspections. Provision shall be made for free access by regulatory inspectors to any facility or activity, at any time, within the constraints of ensuring operational safety at all times and other constraints associated with the potential for harmful consequences. These inspections may include, within reason, unannounced inspections. The manner, extent and frequency of inspections shall be in accordance with a graded approach. 4.53. In conducting inspections, the regulatory body shall consider a number of aspects, including: —Structures, systems and components and materials important to safety; —Management systems; —Operational activities and procedures; —Records of operational activities and results of monitoring; —Liaison with contractors and other service providers; —Competence of staff; —Safety culture; —Liaison with the relevant organization for joint inspections, where necessary.		
132	4	Requirement 33: Review of regulations and guides	Regulations and guides shall be reviewed and revised as necessary to keep them up to date, with due consideration of relevant international safety standards and technical standards and of relevant experience gained.			

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
133	4	Requirement 34: Promotion of regulations and guides to interested parties	The regulatory body shall notify interested parties and the public of the principles and associated criteria for safety established in its regulations and guides, and shall make its regulations and guides available.	4.61. The government or the regulatory body shall establish, within the legal framework, processes for establishing or adopting, promoting and amending regulations and guides. These processes shall involve consultation with interested parties in the development of the regulations and guides, with account taken of internationally agreed standards and the feedback of relevant experience. Moreover, technological advances, research and development work, relevant operational lessons learned and institutional knowledge can be valuable and shall be used as appropriate in revising the regulations and guides. 4.62. The regulations and guides shall provide the framework for the regulatory requirements and conditions to be incorporated into individual authorizations or applications for authorization. They shall also establish the criteria to be used for assessing compliance. The regulations and guides shall be kept consistent and comprehensive, and shall provide adequate coverage commensurate with the radiation risks associated with the facilities and activities, in accordance with a graded approach.		
134	4	Requirement 35: Safety related records	The regulatory body shall make provision for establishing, maintaining and retrieving adequate records relating to the safety of facilities and activities.	4.63. The regulatory body shall make provision for establishing and maintaining the following main registers and inventories: —Registers of sealed radioactive sources and radiation generators;10 —Records of doses from occupational exposure; —Records relating to the safety of facilities and activities; —Records that might be necessary for the shutdown and decommissioning (or closure) of facilities; —Records of events, including non-routine releases of radioactive material to the environment; —Inventories of radioactive waste and of spent fuel. 4.64. The regulatory body may or may not be the sole entity responsible for the maintenance of these registers and inventories, but it shall be involved in their proper retention and use. The authorized party shall be responsible for maintaining its own records. The authorized party shall maintain all the records necessary for the safe operation of facilities and the safe conduct of activities, as specified in the authorization. This includes maintaining an inventory of radioactive sources and inventories of radioactive waste and of spent fuel, as well as records of doses from occupational exposure. The requirement for the regulatory body to maintain records cannot diminish the responsibility of authorized parties to keep their own records. 4.65. Applicants shall be responsible for ensuring the recording of information relating to facilities and activities in registers and inventories, and analysing it, where relevant, for the purposes of demonstrating safety. Moreover, the regulatory body shall use such records in support of its regulatory functions and to support the enforcement of regulatory requirements.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
135	4	Requirement 36: Communication and consultation with interested parties	The regulatory body shall promote the establishment of appropriate means of informing and consulting interested parties and the public about the possible radiation risks associated with facilities and activities, and about the processes and decisions of the regulatory body.	4.66. The regulatory body shall establish, either directly or through authorized parties, provision for effective mechanisms of communication, and it shall hold meetings to inform interested parties and the public and for informing the decision making process. This communication shall include constructive liaison such as: (a) Communication with interested parties and the public on regulatory judgements and decisions; (b) Direct communication with governmental authorities at a high level when such communication is considered necessary for effectively performing the functions of the regulatory body; (c) Communication of such documents and opinions from private or public organizations or persons to the regulatory body as may be considered necessary and appropriate; (d) Communication on the requirements, judgements and decisions of the regulatory body, and on the bases for them, to the public; (e) Making information on incidents in facilities and activities, including accidents and abnormal events, and other information, as appropriate, available to authorized parties, governmental bodies, national and international organizations, and the public. 4.67. The regulatory body, in its public informational activities and consultation, shall set up appropriate means of informing interested parties, the public and the news media about the radiation risks associated with facilities and activities, the requirements for protection of people and the environment, and the processes of the regulatory body. In particular, there shall be consultation by means of an open and inclusive process with interested parties residing in the vicinity of authorized facilities and activities, and other interested parties, as appropriate [1]. Interested parties including the public shall have an opportunity to be consulted in the process for making significant regulatory decisions, subject to national legislation and international obligations. The results of these consultations shall be taken into consideration by the regulatory body in a transparent manner. 4.68. The authorized party shall inform the public about the possible radiation risks (arising from operational states and accidents, including events with a very low probability of occurrence) associated with the operation of a facility or the conduct of an activity. This obligation shall be specified in the regulations promulgated by the regulatory body, in the authorization or by other legal means. 4.69. Public information activities shall reflect the radiation risks associated with facilities and activities, in accordance with a graded approach.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
144	5	Principle 9: Emergency preparedness and response	Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents.	3.34. The primary goals of preparedness and response for a nuclear or radiation emergency are: —To ensure that arrangements are in place for an effective response at the scene and, as appropriate, at the local, regional, national and international levels, to a nuclear or radiation emergency; —To ensure that, for reasonably foreseeable incidents, radiation risks would be minor; —For any incidents that do occur, to take practical measures to mitigate any consequences for human life and health and the environment. 3.35. The licensee, the employer, the regulatory body and appropriate branches of government have to establish, in advance, arrangements for preparedness and response for a nuclear or radiation emergency at the scene, at local, regional and national levels and, where so agreed between States, at the international level. 3.36. The scope and extent of arrangements for emergency preparedness and response have to reflect: —The likelihood and the possible consequences of a nuclear or radiation emergency; —The characteristics of the radiation risks; —The nature and location of the facilities and activities. Such arrangements include: —Criteria set in advance for use in determining when to take different protective actions; —The capability to take actions to protect and inform personnel at the scene, and if necessary the public, during an emergency. 3.37. In developing the emergency response arrangements, consideration has to be given to all reasonably foreseeable events. Emergency plans have to be exercised periodically to ensure the preparedness of the organizations having responsibilities in emergency response. 3.38. When urgent protective actions must be taken promptly in an emergency, it may be acceptable for emergency workers to receive, on the basis of informed consent, doses that exceed the occupational dose limits normally applied — but only up to a predetermined level.	Lack of preparedness to manage events after an accident to minimize impacts to the public Lack of preparedness for all reasonably foreseeable accidents	Processes in place to manage all reasonably foreseeable accidents to minimize impacts to the public

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
145	5	Principle 10: Protective actions to reduce existing or unregulated radiation risks	Protective actions to reduce existing or unregulated radiation risks must be justified and optimized.	3.39. Radiation risks may arise in situations other than in facilities and activities that are in compliance with regulatory control. In such situations, if the radiation risks are relatively high, consideration has to be given to whether protective actions can reasonably be taken to reduce radiation exposures and to remediate adverse conditions. —One type of situation concerns radiation of essentially natural origin. Such situations include exposure to radon gas in dwellings and workplaces, for example, for which remedial actions can be taken if necessary. However, in many situations there is little that can practicably be done to reduce exposure to natural sources of radiation. —A second type of situation concerns exposure that arises from human activities conducted in the past that were never subject to regulatory control, or that were subject to an earlier, less rigorous regime of control. An example is situations in which radioactive residues remain from former mining operations. —A third type of situation concerns protective actions, such as remediation measures, taken following an uncontrolled release of radionuclides to the environment. 3.40. In all of these cases, the protective actions considered each have some foreseeable economic, social and, possibly, environmental costs and may entail some radiation risks (e.g. to workers carrying out such actions). The protective actions are considered justified only if they yield sufficient benefit to outweigh the radiation risks and other detriments associated with taking them. Furthermore, protective actions must be optimized to produce the greatest benefit that is reasonably achievable in relation to the costs.	Lack of preparedness for events that impact public safety that are beyond the specific legislation and regulations in place.	Risks beyond those specifically addressed in legislation and regulation are taken into account in emergency preparedness

153	6	3.3.2. Quality assurance	Principle: Quality assurance is applied throughout activities at a nuclear power plant as part of a comprehensive system to ensure with high confidence that all items delivered and services and tasks performed meet specified requirements.	76. The comprehensive system referred to in the principle begins with analysis and design in accordance with the preceding principle on proven engineering, and it continues with the use of quality assurance methods. Other fundamental technical safety principles are also important in this respect, particularly those on safety assessment and verification and on operating experience and safety research. 77. High quality in equipment and in human performance is at the heart of nuclear plant safety. The goal is to ensure that equipment will function and individuals will perform in a satisfactory way. The processes in which high quality is sought are subject to control and verification by quality assurance practices. Throughout the lifetime of the plant, these practices apply to the entire range of activities in design, supply and installation, and to the control of procedures in plant testing, commissioning, operation and maintenance. 78. All safety related components, structures and systems are classified on the basis of their functions and significance with regard to safety, and they are so designed, manufactured and installed that their quality is commensurate with that classification (see paras 161 and 182–185). 79. Quality assurance practices are a component of good management and are essential to the achievement and demonstration of high quality in products and operation. Organizational arrangements for sound quality assurance practices are requisite for all parties concerned, to provide a clear definition of the responsibilities and authorities of component groups and channels of communication and co-ordination between them. These arrangements are founded on the principle that the responsibility for achieving quality in a task rests with those performing it, others verify that the task has been properly performed, and yet others audit the entire process. The authority of the quality assurance staff is established firmly enough within the organization to allow them to identify problems of inadequate quality and to solve them. The selection and training of staff for quality assurance duties, adapted appropriately to national cultural and technical norms, receives special attention. 80. Quality assurance programmes provide a framework for the analysis of tasks, development of methods, establishment of standards and identification of necessary skills and equipment. Within this framework is the definition of the items and activities to which quality assurance applies and the standards or other requirements to be implemented through instructions, calculations, specifications, drawings and other statements. 81. Quality assurance practices thus cover: validation of designs; procurement; supply and use of materials; manufacturing, inspection and testing methods; and operational and other procedures to ensure that specifications are met. The associated documents are subject to strict procedures for verification, issue, amendment and withdrawal. Formal arrangements for handling of variations and deviations are an important aspect of quality assurance programmes. 82. An essential component of quality assurance is the documentary verification that tasks have been performed as required, that deviations have been identified and corrected, and that action has been taken to prevent the recurrence of errors. The necessary facilities are provided for this, including a hierarchy of documentation, quality control procedures which provide sampling of work	Quality assurance applied does not provide an adequate level of confidence that the safety requirements and objectives were met	Quality assurance applied to ensure with high level of confidence that safety requirements and objectives are met

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				products, opportunity for observation of actual practices and witnessing of tests and inspections, and sufficient staff and other resources.		
154	6	3.3.3. Self-assessment	Principle: Self-assessment for all important activities at a nuclear plant ensures the involvement of personnel performing line functions in detecting problems concerning safety and performance and solving them.	84. Self-assessment is a structured, objective and visible process whereby individuals, groups and management within an operating organization evaluate the effectiveness of their own operational safety measures against pre-established expectations and identify areas needing improvement. Those individuals involved in the activities being reviewed can improve the objectivity of the self-assessment through the participation of persons independent of the activities. The results are used to complement quality assurance audits and safety reviews conducted by independent personnel (i.e. those who are not directly involved in the tasks being performed). Self-assessments are used for single reviews in depth to find the basic causes of poor safety and performance; for periodic reviews of specific activities or programmes by teams of experienced in-house personnel and outside technical experts; for comparison of plant performance with existing management expectations and with best industry practices; and for frequent or continuous monitoring of activities at all levels of the entire organization. Strong support from management is essential to obtaining good results and to encouraging individuals at all levels of the organization to employ self-evaluation to improve performance rather than just solve problems. 85. Self-assessment reports are clear and deal with the problems found, their root causes and their generic implications. Corrective actions are tracked to completion and their effectiveness is verified in subsequent self-assessments. The involvement of individuals engaged in or responsible for the activity being reviewed is valuable in that it brings their knowledge and insights to the review process. Those individuals also gain understanding and valuable perspectives that can help them to assess and improve their own performance in their areas of responsibility.	Safety related activities that are not being performed adequately are not identified and corrected.	Self-assessment used to evaluate effectiveness of processes against pre-established expectations Areas needing improvement are identified and the corrective actions tracked to completion

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
155	6	3.3.4. Peer reviews	Principle: Independent peer reviews provide access to practices and programmes employed at plants performing well and permit their adoption at other plants.	87. 'Peer reviews' are conducted by a team of independent experts with technical competence and experience in the areas of evaluation. Judgements are based on the combined expertise of the team members. The composition of the team is tailored to the organization to be reviewed. Depending on specific needs, the review process can address general topics or concentrate on specific areas of special interest. The scope of this process is not limited to examination of documents or to interviews; it emphasizes plant performance. These reviews are neither inspections nor audits against specified standards. Instead, they comprise a comprehensive comparison of the practices applied by organizations with existing and internationally accepted good practices, and an exchange of expert judgements. They are aimed at increasing the effectiveness of practices and procedures of the organization being reviewed. 88. Peer reviews are themselves a 'good practice', complementing other types of assessment. Peer reviews are carried out at the national, bilateral and/or multilateral or international level, and they cover operating organizations as well as regulatory authorities. International organizations typically performing operational peer reviews are the World Association of Nuclear Operators (WANO) and the IAEA through its Operational Safety Review Teams.	Safety related activities that are not being performed adequately are not identified and corrected.	Peer review used to identify areas for improvement

157	6	3.3.6. Safety assessment and verification	Principle: Safety assessment is made before construction and operation of a plant begin. The assessment is well documented and independently reviewed. It is subsequently updated in the light of significant new safety information.	97. Safety assessment includes systematic critical review of the ways in which structures, systems and components might fail, and identifies the consequences of such failures. The assessment is undertaken expressly to reveal any underlying design weaknesses. The results are documented in detail to allow independent audit of the scope, depth and conclusions of the critical review. The safety analysis report prepared for licensing contains a description of the plant sufficient for independent assessment of its safety features. It includes information on the features of the site that the design must accommodate. It provides detailed information on the major features of systems, especially of those systems used in reactor control and shutdown, cooling, the containment of radioactive material and particularly the engineered safety features. It provides the technical rationale for selection of, and describes the limiting set of design basis accidents and presents the results. 98. The safety analysis report and its review by the regulatory authorities constitute a principal basis for the approval of construction and operation, demonstrating that all safety questions have been adequately resolved or are amenable to resolution. 99. Methods have been developed to assess whether safety objectives are met. These methods are applied at the design stage, later in the lifetime of the plant if changes to plant configuration are planned, and in the evaluation of operating experience to verify the continued safety of the plant. Two complementary methods, deterministic and probabilistic, are currently in use. These methods are used jointly in evaluating and improving the safety of design and operation. 100. In the deterministic method, design basis events are chosen to encompass a range of related possible initiating events that could challenge the safety of the plant. Analysis is used to show that the response of the plant and its safety systems to design basis events satisfies predetermined specifications both for the performance of the plant itself and for meeting safety targets. The deterministic method uses accepted engineering analysis to predict the course of events and their consequences. 101. Probabilistic analysis is used to evaluate the likelihood of any particular sequence and its consequences. This evaluation may take into account the effects of mitigation measures inside and outside the plant. Probabilistic analysis is used to estimate risk and especially to identify the importance of any possible weakness in design or operation or during potential accident sequences that contribute to risk. The probabilistic method can be used to aid in the selection of events requiring deterministic analysis and the other way around. 102. Generic or plant specific PSAs are used increasingly to evaluate multiple failure situations and severe accidents. The process employs realistic assumptions and best estimate analyses. The analyses quantify available safety margins and they lead to nuclear plant design changes to reduce the likelihood of radioactive releases and their consequences. A summary of the extensive actions taken in various operating water cooled plants is shown in Table II. For future plants, deterministic and probabilistic safety assessments will be applied to attain the objectives of paras 25 and 27. 103. The safety assessment process is repeated in whole or in part as needed later in the plant's lifetime if ongoing safety research and operating experience make	Plant construction begins before agreement is achieved with the regulator on the assessment of plant safety. The safety assessment is not well documented and not independently reviewed.	Safety assessment done before construction and operation begins Safety assessment is performed independently and documented in a third party reviewable manner

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				this possible and advisable. For example, a large number of requirements are specified for the surveillance test interval and allowed outage time for plant components and systems. PSA is being used to identify the components important to risk and to adjust the requirements for important components to be consistent with their risk contribution.		
158	6	3.3.7. Radiation protection	Principle: A system of radiation protection practices, consistent with recommendations of the ICRP and the IAEA, is followed in the design, commissioning, operational and decommissioning phases of nuclear power plants.	105. Measures are taken to protect workers and the public against the harmful effects of radiation in normal operation, anticipated operational occurrences and accidents. These measures are directed towards control of the sources of radiation, including radioactive releases and waste; to the provision and continued effectiveness of protective barriers and personal protective equipment; and to the provision of administrative means for controlling exposures. 106. Radiation protection is considered in the design process by paying attention to both specific details and broad aspects of plant layout. 107. For the control, guidance and protection of personnel, procedures are written which define safe practices, the physical means of protection and the necessary administrative procedures for each task which might lead to the exposure of personnel to radiation. Special attention is given to dose intensive work. 108. These are the principal features that make it possible to meet the radiation protection objective. To ensure that it is met calls for continued vigilance, monitoring of plant conditions and the maintenance of a clean orderly plant.	Radiation protection practices are inconsistent with ICRP and IAEA recommendations	Radiation protection practices are consistent with ICRP and IAEA recommendations

159	6	3.3.8. Operating experience and safety research	Principle: Organizations concerned ensure that operating experience and the results of research relevant to safety are exchanged, reviewed and analysed, and that lessons are learned and acted on.	110. The organization operating a nuclear power plant maintains an effective system for collection and interpretation of operating experience, and it disseminates safety significant information promptly among its own staff and to other relevant organizations. The root causes of accidents are analysed. Events that may be regarded as precursors of accidents are identified and actions are taken to prevent any recurrence. Each operating organization seeks to learn from the experience of other organizations. The sharing of operating data is co-ordinated nationally and internationally. 111. The primary objective is that safety shortfalls are recognized and that corrections are made to prevent the recurrence, either at the same location or elsewhere, of safety related abnormal events, no matter where they first occurred. Most importantly, this principle reflects the point that an accident of any severity would most probably be marked by precursor events, and to this extent would be predictable and therefore avoidable. Feedback of experience also increases knowledge of the operating characteristics of equipment and performance trends, and provides data for numerical safety analysis. 112. Many operating organizations have a programme of gathering information specific to their plants and using it to trend and improve the plant performance. The accumulated information is on reported plant events, errors, near misses, problems, observations, and even suggestions for improvement. The information is reviewed by representatives from different plant functions and it is assigned a safety significance level. The important safety issues are investigated promptly and are subjected to root cause analysis before corrective actions are taken. Operational errors are considered important and are evaluated separately. A process is established to track the various assessments and corresponding corrective actions and to determine unfavourable trends, which can be reversed. Management involvement in this internal programme of information gathering and satisfactory resolution of issues is essential to success. The key to a good and substantive programme is whether employees are willing to report problems and suggest improvements. 113. Research to understand nuclear power plant performance, the response to abnormal occurrences and the possible sequences of events in severe accidents leads to improved interpretation of experience and better definition of corrective measures that might be necessary. Further advantages are gained by the use of research results to improve plant performance while still keeping acceptable safety margins. Results of research may be incorporated into nuclear power plant design, helping to make these plants still safer. More generally, research and development activities are needed to maintain knowledge and competence within organizations that support or regulate nuclear power plant activities. 114. Research efforts clearly enhance the safety of nuclear power plants and reduce the prevailing uncertainties in predicting their performance or the consequences of accidents. The scope of research and development programmes is broad so as to cover all areas of interest, including potential modifications to existing designs. The work ranges from investigating degradation mechanisms to the development of structural materials more resistant to corrosion; the qualification of fuel for extended burnup or with mixed oxide (MOX) fissionable material; the introduction of improved coolant chemistry to improve plant reliability and to reduce the impact of ageing; the	Safety related activities that are not being performed adequately are not identified and corrected. Operating experience and relevant research is not being used to identify areas for improvement.	Operating experience and research relevant to safety is used to identify areas for improvement to safety

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				development of system computer codes to predict plant performance during transients and in accidents and severe accidents and to reduce the uncertainties in previous safety analyses; the introduction of improved and computerized control systems and instrumentation to simplify the human–machine interface; and the development of a more realistic set of possible radioactive releases for predicting the consequences of severe accidents. Nuclear research and development is an essential element of nuclear plant safety and its continued support is very important. However, there is a need to prioritize research and development work with respect to its safety significance. Also, co-operative research on an international scale to reach a common understanding on major safety issues is an important way to avoid duplication of efforts and to reduce costs.		
165	6	4.2.1.1. Design management	Principle: The assignment and subdivision of responsibility for safety are kept well defined throughout the design phase of a nuclear power plant project, and during any subsequent modifications.	151. The design of a safe plant is under the authority of a highly qualified engineering manager whose attitudes and actions reflect a safety culture and who ensures that all safety and regulatory requirements are met. Separate aspects of design may be served by different sections of a central design group and by other groups subcontracted to specific parts of the project. An adequate number of qualified personnel for each activity are essential. The engineering manager establishes a clear set of interfaces between the groups engaged in different parts of the design, and between designers, suppliers and constructors. 152. The design force is engaged in the preparation of safety analysis reports and other important safety documents. It also includes a co-ordinating group that has the responsibility of ensuring that all safety requirements are fulfilled. This group remains familiar with the features and limitations of components included in the design. It communicates with the future operating staff to ensure that requirements from that source are recognized in the design and that there is appropriate input from the designer to the operating procedures as they are prepared and to the planning and conduct of training. It has direct access to the design manager but does not necessarily report to that manager. 153. In accordance with the fundamental principle of Section 3.3.2, quality assurance is carried out for all design activities important to safety. An essential component of this activity is configuration control, to ensure that the safety design basis is effectively recorded at the start and then kept up to date when design changes occur.	The responsibility for safety is not well defined throughout the design phase and during any subsequent modifications	The assignment and subdivision of responsibility for safety are kept well defined throughout the design phase of a nuclear power plant project, and during any subsequent modifications.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
197	6	4.5.2. Safety review procedures	Principle: Safety review procedures are maintained by the operating organization to provide a continuing surveillance and audit of plant operational safety and to support the plant manager in the overall safety responsibilities.	270. Among the regular activities at the plant there is a line process of safety management which covers all aspects of day to day operations and reports to the plant management. Beyond this, the operating organization provides means for independent safety review, from within the organization itself or with assistance from specialist institutions or other bodies. The principal objective is to ensure that, in those matters that are important for safety, the plant manager will be supported in his accountability by arrangements that are independent of the pressures of plant operation. However this independent review is performed, it is an activity that is separate from plant operation, and that provides safety review on a continuing basis to verify that plant management establishes sound practices and adheres to requirements. The reports from this activity are formal and are provided directly to senior management in the operating organization. Particular attention is paid in these processes to the feedback of experience; the examination of abnormal events and reported plant deficiencies both locally and at similar plants; reviews of validity and modification of operating procedures; safety related plant modifications; training and qualification of staff; response to regulatory requirements; and the general attitudes of management and staff towards the safety of the plant. 271. Most particularly, in individual matters of special safety importance, such as intended abnormal plant manoeuvres, unusual tests or experiments, major plant engineering, or changes in safety limits or conditions, special procedures are first formulated by the line operating and safety staff, and these are subject to the independent review process as part of the mechanism of obtaining formal approval.	Safety related activities that are not being performed adequately are not identified and corrected.	Safety management program in place that covers all day to day operations Ongoing, independent safety reviews in place

199	6	4.5.4. Training	Principle: Programmes are established for training and retraining operations and maintenance, technical support, chemistry and radiation protection personnel to enable them to perform their duties safely and efficiently. Training is particularly intensive for control room staff, and includes the use of plant simulators.	279. The training programme includes the identification of training requirements, the development of training specifications and materials, programme implementation and evaluation. Formal training of operators, maintenance, technical support, chemistry and radiation protection personnel, covers such key areas of technology as neutronics, thermal hydraulics and radiation protection, to the level necessary for the task to be performed. Operator training develops knowledge of the plant and its operation, both theoretically and practically. It includes thorough knowledge of the plant's layout, the locations of important components and systems, the locations and functions and effects of their controls, and the normal line-up of plant systems. Emphasis is placed on systems having safety significance. Trainees learn routines for normal operation of the plant, and the plant's response to the onset of faults that could cause damaging accidents if not counteracted. This aspect of training is aimed at improving diagnostic skills. Training covers lessons learned from operating experience both locally and elsewhere. Operators learn both normal and emergency operating procedures. The operator training programme includes desk studies, use of simulators, on the job training and plant familiarization, leading to formal approval of operators (e.g. by licensing). 280. Through the training programmes, operators, maintenance, technical support, chemistry and radiation protection personnel are apprised of the principal results of any PSAs of the plant, showing the importance of plant systems in preventing plant damage or severe accidents. They are aware of the locations of all significant amounts of radioactive material in the plant, and understand the measures to prevent its dispersal. Most importantly, the training of operating staff emphasizes the importance of maintaining the plant within its operational limits and conditions. The consequences of violating limits are emphasized. The importance is stressed of maintaining subcriticality when the plant is not operating, of continued core cooling at all times, and of the controlled retention of all radioactive materials. Continuous training is provided at intervals to ensure that knowledge and understanding essential to safe and efficient plant operation are retained and refreshed, in particular for handling abnormal and accident conditions. Structured initial training and refresher training are given on a representative simulator. Team work is emphasized in operator training, particularly in simulator exercises on dealing with incidents and accidents. 281. Complementary training is provided to prepare staff for specialized duties required in the event of an accident. In judging the need for and extent of such training, standby arrangements and the availability of off-site services are taken into account. Specific training is provided for all staff members who have assignments under the emergency plans. 282. Training of maintenance staff goes beyond the teaching of basic task skills to emphasize the potential safety consequences of technical or procedural error. Training and qualification of maintenance staff reflects the realization that where there has been a record of plant operational unreliability and faulty, spurious and accidental activation of safety systems in the past, it has often been caused by errors in maintenance procedures and practices. Training of maintenance staff covers such incidents. Testing of maintenance staff examines their familiarity with these lessons. Training of technical support, chemistry, radiation protection and other staff recognizes the safety importance of their duties.	Safety related activities are not being performed adequately due to lack of adequate competencies of operations, maintenance and support staff.	Training programs in place to ensure that personnel responsible for safety related tasks have the necessary competencies

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				283. The training of senior operations and management staff emphasizes the special problems of managing a nuclear power plant, with the exceptional demand for safety and the need for familiarity with emergency procedures. The training also includes discussion of operating experience and of the management/supervisor role in enforcing operational standards and practices.		
201	6	4.5.6. Normal operating procedures	Principle: Normal plant operation is controlled by detailed, validated and formally approved procedures.	289. Plant operating procedures are based on plant design and safety analysis and validated by computer simulation, plant commissioning and the feedback of operating experience. They are presented in sufficient detail to permit the operators to perform plant operations without their further elaboration. From the safety standpoint, the procedures, if properly followed, ensure that the plant's operational limits or conditions are not exceeded and that the necessary safety related components, systems and structures are available. Specifications included in the procedures cover periodic testing, periodic calibration and periodic inspection of safety systems. Particular attention is given in these procedures to changes of operational states, low power operation, test conditions and occasions when parts of safety systems may be unavailable by intent. In the procedures for core loading and unloading, attention is given to avoiding unplanned criticality or other accidents that could occur. Operating procedures are revised only after approval in accordance with established procedures, and the documents that define the operating procedures are subject to managerial control in accordance with quality assurance procedures. Operators are trained on major revisions to operating procedures prior to their implementation. Special controls and procedures are implemented for special tests.	Safety related activities are not being performed adequately due to lack of adequate operating procedures.	Normal plant operations are controlled by detailed, validated and formally approved procedures
202	6	4.5.7. Emergency operating procedures	Principle: Emergency operating procedures are established, documented and approved to provide a basis for suitable operator response to abnormal events.	291. The engineered systems installed to take care of abnormal events within the design basis of the plant would be actuated automatically upon initiation of any such event. The operating staff are trained to take advantage of the period identified in the design as 'requiring no immediate operator action' to detect and identify the causes of the automatic response. Additional information conveyed to the operators by instruments and display systems would help them in deciding on action to prevent or mitigate plant damage. Also, emergency operating procedures are available for accidents taken into account in the design and for any accidents beyond the design basis that are considered to contribute significantly to risk. These procedures generally embody responses based on a diagnosis of the event occurring. If the event cannot be diagnosed in time, or if further evaluation of the event causes the initial diagnosis to be discarded, the emergency operating procedures define responses to the symptoms observed, from knowledge less of the nature of the event itself than of the plant conditions arising as deduced from these symptoms. Actions based on symptom oriented procedures are designed to restore critical safety functions. The emergency operating procedures also facilitate long term recovery from an accident and limitation of its radiological consequences for the plant personnel and the public. These procedures are part of the training programme of operating and radiation protection staff. They include ultimate emergency procedures to facilitate management of severe accidents.	Emergency operating activities are not being performed adequately due to lack of adequate emergency operating procedures.	Emergency operating procedures established for abnormal events

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
203	6	4.5.8. Radiation protection procedures	Principle: The radiation protection staff of the operating organization establish written procedures for the control, guidance and protection of personnel, carry out routine monitoring of in-plant radiological conditions, monitor the exposure of plant personnel to radiation, and also monitor releases of radioactive effluents.	293. Specialist staff under the control of the plant management provide a comprehensive radiation protection service. This covers personnel monitoring and dose records, measurement of radiation levels in key areas, measurement of radiological effluents from the plant, monitoring the cleanup of contamination and the preparation of radioactive waste for storage or disposal, and supervision and monitoring of the entry of personnel into radiation areas. The radiation monitoring staff also have assigned responsibilities in the event of emergencies. Following appropriate training members of the operating staff may assume some of these radiation protection duties. Written procedures are issued as necessary to cover radiation protection functions. 294. The radiation protection staff have direct access to senior plant management as necessary to advise on and secure the observance of radiation protection procedures. Individual workers are motivated by the management and by the radiation protection staff to control their own dose and exposure and to keep their own routine radiation exposures as low as practicable. 295. Special equipment is provided to assist in radiation protection for some in-plant maintenance and surveillance activities. This is especially important for safety related systems: the possibility of personnel exposures must not be allowed to reduce the care taken of the safety systems. Workers who must perform tasks under conditions of high dose rates are trained in the use of special equipment and with mockups of the systems to be serviced.	Radiation protection activities are not being performed adequately due to lack of adequate procedures.	Operating organization established procedures for radiation protection staff

206	6	4.5.11. Maintenance, testing and inspection	Principle: Safety related structures, components and systems are the subject of regular preventive and predictive maintenance, inspection, testing and servicing when needed, to ensure that they remain capable of meeting their design requirements throughout the lifetime of the plant. Such activities are carried out in accordance with written procedures supported by quality assurance measures.	306. When a nuclear plant goes into operation, regular and scheduled preventive maintenance and surveillance are begun to ensure that structures, components and systems continue to operate as desired, with their capability to meet the design objectives undiminished by ageing, wear or other deterioration. Trend analysis (e.g. of wear and vibration) is used to improve the effectiveness of the programme. These activities play an essential role in preventing failures in subsequent operation. Deficiencies thus detected are corrected in a timely fashion. Conformity to written and approved procedures is required where important safety related systems are concerned. The procedures ensure that the control room staff remain informed of the status of any such work under way. 307. An approved schedule of inspection is followed, based on assessment at the design stage and testing during commissioning, and it is modified according to experience. Special attention is devoted to the surveillance of the multibarrier system, in particular the primary coolant boundary, which is subject to neutron irradiation, thermal and pressure cycling and ageing as a normal consequence of use. Where necessary, use is made of tests performed on removable samples that have been exposed to service conditions. Maintenance activities are planned and executed in recognition of the importance of safety related systems and bearing in mind the possibility that imprudent maintenance practices can reduce the potential benefit of defence in depth. 308. A major component of reassurance that essential safety functions are available when called upon is the periodic functional testing of safety systems. The frequency, extent and nature of such testing is determined by the reliability required, and by the practical capability to simulate the function. In circumstances where full demonstration is not possible in periodic testing, testing of individual components and partial systems is performed to demonstrate the reliability of the safety function. 309. Since incorrectly performed maintenance and testing can cause problems, consideration is given to the optimization of such maintenance features as the frequency and extent of preventive maintenance, and to instructions from equipment manufacturers, operating experience and trend analysis, training and procedures. 310. Radiation exposure of personnel during maintenance is controlled and limited by means of work plans, rehearsals and monitoring for radiation control. 311. Achieving high safety standards in maintenance requires that key maintenance personnel be aware of the safety aspects of the tasks they are performing. Maintenance workers are therefore carefully prepared for their duties to reduce the possibility of human error in these cases. Maintenance sometimes requires disabling particular safety systems. This is only permitted if carefully written, tested and approved procedures are followed and compensatory measures taken, in accordance with Section 4.5.5. The associated risk is assessed and found acceptable. Maintenance staff are trained on the particular equipment that they service. When work is performed on equipment by individuals who are not members of the trained and qualified plant staff, it is supervised and checked by on-site personnel who have been fully trained in the performance and significance for safety of the work and who are themselves qualified to perform it.	Programme for inspection, maintenance and testing is inadequate to ensure that safety related systems perform in accordance with their safety requirements.	Safety related structures, system and components are subject to regular maintenance, inspection and testing as necessary to ensure that they perform consistent with safety requirements over the life of the plant

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
207	6	4.5.12. Quality assurance in operation	Principle: An operational quality assurance programme is established by the operating organization to assist in ensuring satisfactory performance in all plant activities important to plant safety.	313. This specific principle fulfils the fundamental principle on quality assurance (Section 3.3.2) for the area of operations. The operational quality assurance programme supports the line managers who are responsible for the quality of work performed, including the plant manager who has responsibility for the safety of the entire plant.	Operational quality assurance applied does not provide an adequate level of confidence that the safety requirements and objectives applicable to safety related operational phase activities are met.	Operational quality assurance program established to ensure that plant activities are performed consistent with pre-established expectations

OPERATIONS AND MAINTENANCE PHASE

Organization

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
41	1	Requirement 3: Safety of the plant design throughout the lifetime of the plant	The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant.	3.5. The formal system for ensuring the continuing safety of the plant design shall include a formally designated entity responsible for the safety of the plant design within the operating organization's management system. Tasks that are assigned to external organizations (referred to as responsible designers) for the design of specific parts of the plant shall be taken into account in the arrangements. 3.6. The formally designated entity shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and regulations. A series of tasks and functions shall be established and implemented to ensure the following: (a) That the plant design is fit for purpose and meets the requirement for the optimization of protection and safety by keeping radiation risks as low as reasonably achievable; (b) That the design verification, definition of engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design; (c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings; (d) That management of design requirements and configuration control are maintained; (e) That the necessary interfaces with responsible designers and suppliers engaged in design work are established and controlled; (f) That the necessary engineering expertise and scientific and technical knowledge are maintained within the operating organization; (g) That all design changes to the plant are reviewed, verified, documented and approved; (h) That adequate documentation is maintained to facilitate future decommissioning of the plant.	Design modification made during the operations phase of the plant result in non-compliance with safety requirements Design modifications made during the operations phase of the plant result in new hazards that are not adequately handled by the design	Clear responsibility for the safety of the plant within the operating organization's management system Establishment of a design modification process that is compliant with relevant national and international standards, and is based on proven engineering practices Establishment of governance that focuses on optimizing safety by keeping radiation risks as low as reasonably achieveable Establishment of governance that focuses on optimizing safety by establishing a safety culture throughout the organization Establishment of controls over the configuration of the physical plant and its design Establishment of controls of the interfaces between responsible designers and suppliers engaged in design work Establishment of a program to establish the necessary competencies required within the operating organization and the development and training program to maintain the required competencies

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
77	2	Requirement 3: Structure and functions of the operating organization	The structure of the operating organization and the functions, roles and responsibilities of its personnel shall be established and documented.	3.8. Functional responsibilities, lines of authority, and lines of internal and external communication for the safe operation of a plant in all operational states and in accident conditions shall be clearly specified in writing. Authority for the safe operation of the plant may be delegated to the plant management. In this case, the necessary resources and support shall be provided. 3.9. Documentation of the plant's organizational structure and of the arrangements for discharging responsibilities shall be made available to the plant staff and, if required, to the regulatory body. The structure of the operating organization shall be specified so that all roles that are critical for safe operation are specified and described. Proposed organizational changes to the structure and associated arrangements, which might be of importance to safety, shall be analysed in advance by the operating organization. Where so required by the State's regulations, proposals for such organizational changes shall be submitted to the regulatory body for approval.	Lack of an individual taking responsibility for some safety related activity	Clear documentation of functional responsibilities, lines of authority, and lines of communications for all safety related activities
78	2	Requirement 4: Staffing of the operating organization	The operating organization shall be staffed with competent managers and sufficient qualified personnel for the safe operation of the plant.	3.10. The operating organization shall be responsible for ensuring that the necessary knowledge, skills, attitudes and safety expertise are sustained at the plant, and that long term objectives for human resources policy are developed and are met. 3.11. The organization, qualifications and number of operating personnel shall be adequate for the safe and reliable operation of the plant in all operational states and in accident conditions. Succession planning shall be an established practice for the operating personnel. The recruitment and selection policy of the operating organization shall be directed at retaining competent personnel to cover all aspects of safe operation. A long term staffing plan aligned to the long term objectives of the operating organization shall be developed in anticipation of the future needs of the operating organization for personnel and skills. 3.12. The shift team shall be staffed to ensure that sufficient authorized operators are present to operate the plant in accordance with the operational limits and conditions. The shift staffing patterns, shift cycles and controls on working hours shall provide sufficient time for the training of shift personnel. Distractions to control room operators shall be minimized. To avoid overburdening control room operators and to allow them to focus on their responsibilities for safety, activities shall be scheduled to reduce simultaneous activities as far as possible. 3.13. A staff health policy shall be instituted and maintained by the operating organization to ensure the fitness for duty of personnel. Attention shall be paid to minimizing conditions causing stress, and to setting restrictions on overtime and setting requirements for rest breaks. The health policy shall cover the prohibition of alcohol consumption and drug abuse.	Personnel involved in safety related activities did not have the competencies to perform the activity adequately Insufficient competent personnel to perform safety related activities Personnel assigned safety related activities were overburdened and hence unable to perform the safety related activities adequately Personnel assigned safety related activities were not fit for duty	Establish a program to ensure personnel assigned to safety related activities have the necessary competencies to perform the activities assigned to them Establish a staffing plan that ensures that sufficient competent staff are available to perform safety related activities Establish policies for scheduling of personnel for safety related activities to ensure that sufficient time is allocated to adequately perform the activities Establish a staff health policy that ensures staff are fit for duty

79	2	Requirement 7: Qualification and training of personnel	The operating organization shall ensure that all activities that may affect safety are performed by suitably qualified and competent persons.	4.16. The operating organization shall clearly define the requirements for qualification and competence to ensure that personnel performing safety related functions are capable of safely performing their duties. Certain operating positions may require formal authorization or a licence. 4.17. Suitably qualified personnel shall be selected and shall be given the necessary training and instruction to enable them to perform their duties correctly for different operational states of the plant and in accident conditions, in accordance with the appropriate procedures. 4.18. The management of the operating organization shall be responsible for the qualification and the competence of plant staff. Managers shall participate in determining the needs for training and in ensuring that operating experience is taken into account in the training. Managers and supervisors shall ensure that production needs do not unduly interfere with the conduct of the training programme. 4.19. A suitable training programme shall be established and maintained for the training of personnel before their assignment to safety related duties. The training programme shall include provision for periodic confirmation of the competence of personnel and for refresher training on a regular basis. The refresher training shall also include retraining provision for personnel who have had extended absences from their authorized duties. The training shall emphasize the importance of safety in all aspects of plant operation and shall promote safety culture. 4.20. Performance based programmes for initial and continuing training shall be developed and put in place for each major group of personnel (including, if necessary, external support organizations, including contractors). The content of each programme shall be based on a systematic approach. Training programmes shall promote attitudes that help to ensure that safety issues receive the attention that they warrant. 4.21. The training programmes shall be assessed and improved by means of periodic review. In addition, a system shall be put in place for the timely modification and updating of the training facilities, computer models, simulators and materials to ensure that they adequately reflect current plant conditions and operating policy, and that any differences are justified. 4.22. Operating experience at the plant, as well as relevant experience at other plants, shall be appropriately incorporated into the training programme. It shall be ensured that training is conducted on the root cause(s) of the events and on the determination and implementation of corrective actions to make their recurrence less likely. 4.23. All training positions shall be held by adequately qualified and experienced persons, who provide the requisite technical knowledge and skills and have credibility with the trainees. Instructors shall be technically competent in their assigned areas of responsibility, shall have the necessary instructional skills, and	Personnel involved in safety related activities did not have the competencies to perform the activity adequately	Clear definitions for the qualifications and competencies of personnel assigned to safety related activities are documented. Governance for assigning personnel to safety related tasks includes confirmation that the personnel have the necessary qualifications and competencies Establishment of a training program that ensures that personnel assigned to safety related tasks have the necessary qualifications and competencies Establishment of a continuous improvement program for the training program

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				shall also be familiar with routines and work practices at the workplace. Qualification requirements shall be established for the training instructors. 4.24. Adequate training facilities, including a representative simulator, appropriate training materials, and facilities for technical training and maintenance training, shall be made available for the training of operating personnel. Simulator training shall incorporate training for plant operational states and for accident conditions.		
80	3	Requirement 9: Provision of resources	Senior management shall determine the competences and resources necessary to carry out the activities of the organization safely and shall provide them.	4.21. Senior management shall make arrangements to ensure that the organization has in-house, or maintains access to, the full range of competences and the resources necessary to conduct its activities and to discharge its responsibilities for ensuring safety at each stage in the lifetime of the facility or activity, and during an emergency response [13, 14, 18].10 4.22. Senior management shall determine which competences and resources the organization has to retain or has to develop internally, and which competences and resources may be obtained externally, for ensuring safety. 4.23. Senior management shall ensure that competence requirements for individuals at all levels are specified and shall ensure that training is conducted, or other actions are taken, to achieve and to sustain the required levels of competence. An evaluation shall be conducted of the effectiveness of the training and of the actions taken. 4.24. Competences to be sustained in-house by the organization shall include: competences for leadership at all management levels; competences for fostering and sustaining a strong safety culture; and expertise to understand technical, human and organizational aspects relating to the facility or the activity in order to ensure safety. 4.25. Senior management shall ensure that individuals at all levels, including managers and workers: (a) Are competent to perform their assigned tasks and to work safely and effectively; (b) Understand the standards that they are expected to apply in completing their tasks. 4.26. All individuals in the organization shall be trained in the relevant requirements of the management system. Such training shall be conducted to ensure that individuals are knowledgeable of the relevance and the importance of their activities and of how their activities contribute to ensuring safety in the achievement of the organization’s goals. 4.27. The knowledge and the information of the organization shall be managed as a resource.	Personnel involved in safety related activities did not have the competencies to perform the activity adequately Insufficient competent personnel to perform safety related activities	Establish a staffing plan that ensures that sufficient competent staff are available to perform safety related activities Establishment of a training program that ensures that personnel assigned to safety related tasks have the necessary qualifications and competencies

103	4	Requirement 4: Independence of the regulatory body	The government shall ensure that the regulatory body is effectively independent in its safety related decision making and that it has functional separation from entities having responsibilities or interests that could unduly influence its decision making.	2.7. An independent regulatory body will not be entirely separate from other governmental bodies. The government has the ultimate responsibility for involving those with legitimate and recognized interests in its decision making. However, the government shall ensure that the regulatory body is able to make decisions under its statutory obligation for the regulatory control of facilities and activities, and that it is able to perform its functions without undue pressure or constraint. 2.8. To be effectively independent from undue influences on its decision making, the regulatory body: (a) Shall have sufficient authority and sufficient competent staff; (b) Shall have access to sufficient financial resources for the proper and timely discharge of its assigned responsibilities; (c) Shall be able to make independent regulatory judgements and regulatory decisions, at all stages in the lifetime of facilities and the duration of activities until release from regulatory control, under operational states and in accidents; (d) Shall be free from any pressures associated with political circumstances or economic conditions, or pressures from government departments, authorized parties or other organizations; (e) Shall be able to give independent advice and provide reports to government departments and governmental bodies on matters relating to the safety of facilities and activities. This includes access to the highest levels of government; (f) Shall be able to liaise directly with regulatory bodies of other States and with international organizations to promote cooperation and the exchange of regulatory related information and experience. 2.9. No responsibilities shall be assigned to the regulatory body that might compromise or conflict with its discharging of its responsibility for regulating the safety of facilities and activities. 2.10. The staff of the regulatory body shall have no direct or indirect interest in facilities and activities or authorized parties6 beyond the interest necessary for regulatory purposes. 2.11. In the event that a department or agency of government is itself an authorized party operating an authorized facility or facilities, or conducting authorized activities, the regulatory body shall be separate from, and effectively independent of, the authorized party. 2.12. Where several authorities are involved in the authorization process, the regulatory requirements shall apply, and they shall be applied consistently and without undue modification. 2.13. The regulatory body shall be conferred with the legal authority to require an authorized party or an applicant, whether a person or an organization, to make arrangements to provide: (a) All necessary safety related information, including information from suppliers, even if this information is proprietary;

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				(b) Access, solely or together with the authorized party or applicant, for making inspections on the premises of any designer, supplier, manufacturer, constructor, contractor or operating organization associated with the authorized party.		
104	4	Requirement 5: Prime responsibility for safety	The government shall expressly assign the prime responsibility for safety to the person or organization responsible for a facility or an activity, and shall confer on the regulatory body the authority to require such persons or organizations to comply with stipulated regulatory requirements, as well as to demonstrate such compliance.			

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
106	4	Requirement 7: Coordination of different authorities with responsibilities for safety within the regulatory framework for safety	Where several authorities have responsibilities for safety within the regulatory framework for safety, the government shall make provision for the effective coordination of their regulatory functions, to avoid any omissions or undue duplication and to avoid conflicting requirements being placed on authorized parties.	2.18. Where several authorities have responsibilities for safety within the regulatory framework for safety, the responsibilities and functions of each authority shall be clearly specified in the relevant legislation. The government shall ensure that there is appropriate coordination of and liaison between the various authorities concerned in areas such as: (1) Safety of workers and the public; (2) Protection of the environment; (3) Applications of radiation in medicine, industry and research; (4) Emergency preparedness and response; (5) Management of radioactive waste (including government policy making and the strategy for the implementation of policy); (6) Liability for nuclear damage (including relevant conventions); (7) Nuclear security; (8) The State system of accounting for, and control of, nuclear material; (9) Safety in relation to water use and the consumption of food; (10) Land use, planning and construction; (11) Safety in the transport of dangerous goods, including nuclear material and radioactive material; (12) Mining and processing of radioactive ores; (13) Controls on the import and export of nuclear material and radioactive material. This coordination and liaison can be achieved by means of memoranda of understanding, appropriate communication and regular meetings. Such coordination assists in achieving consistency and in enabling authorities to benefit from each other's experience. 2.19. If responsibilities and functions do overlap, this could create conflicts between different authorities and lead to conflicting requirements being placed on authorized parties or on applicants. This, in turn, could undermine the authority of the regulatory body and cause confusion on the part of the authorized party or the applicant.		
115	4	Requirement 16: Organizational structure of the regulatory body and allocation of resources	The regulatory body shall structure its organization and manage its resources so as to discharge its responsibilities and perform its functions effectively; this shall be accomplished in a manner commensurate with the radiation risks associated with facilities and activities.	4.4. Requirement 3 establishes that the government shall be responsible for ensuring that the regulatory body has sufficient resources to fulfil its statutory obligations. 4.5. The regulatory body has the responsibility for structuring its organization and managing its available resources so as to fulfil its statutory obligations effectively. The regulatory body shall allocate resources commensurate with the radiation risks associated with facilities and activities, in accordance with a graded approach. Thus, for the lowest associated radiation risks, it may be appropriate for the regulatory body to exempt a particular activity from some or all aspects of regulatory control; for the highest associated radiation risks, it may be appropriate for the regulatory body to carry out a detailed scrutiny in relation to any proposed facility or activity before it is authorized, and also subsequent to its authorization.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
116	4	Requirement 17: Effective independence in the performance of regulatory functions	The regulatory body shall perform its functions in a manner that does not compromise its effective independence.	4.6. Requirements 3 and 4 in Section 2 stipulate that the government establish and maintain a regulatory body that is effectively independent in its decision making and that has functional separation from entities having responsibilities or interests that could unduly influence its decision making. This imposes an obligation on the regulatory body to discharge its responsibilities in such a way as to preserve its effective independence. The staff of the regulatory body shall remain focused on performing their functions in relation to safety, irrespective of any personal views. The competence of staff is a necessary element in achieving effective independence in decision making by the regulatory body. 4.7. The regulatory body shall prevent or duly resolve any conflicts of interests or, where this is not possible, shall seek a resolution of conflicts within the governmental and legal framework. 4.8. To maintain the effective independence of the regulatory body, special consideration shall be given when new staff members are recruited from authorized parties, and the independence of the regulatory body, regulatory aspects and safety considerations shall be emphasized in their training. The regulatory body shall ensure that its staff operate professionally and within its remit in relation to safety. 4.9. To maintain its effective independence, the regulatory body shall ensure that, in its liaison with interested parties, it has a clear separation from organizations or bodies that have been assigned responsibilities for facilities or activities or for their promotion. 4.10. The regulatory body, consistent with its effective independence, shall exercise its authority to intervene in connection with any facilities or activities that present significant radiation risks, irrespective of the possible costs to the authorized party.		
117	4	Requirement 18: Staffing and competence of the regulatory body	The regulatory body shall employ a sufficient number of qualified and competent staff, commensurate with the nature and the number of facilities and activities to be regulated, to perform its functions and to discharge its responsibilities.	4.11. The regulatory body has to have appropriately qualified and competent staff. A human resources plan shall be developed that states the number of staff necessary and the essential knowledge, skills and abilities for them to perform all the necessary regulatory functions. 4.12. The human resources plan for the regulatory body shall cover recruitment and, where relevant, rotation of staff in order to obtain staff with appropriate competence and skills, and shall include a strategy to compensate for the departure of qualified staff. 4.13. A process shall be established to develop and maintain the necessary competence and skills of staff of the regulatory body, as an element of knowledge management. This process shall include the development of a specific training programme on the basis of an analysis of the necessary competence and skills. The training programme shall cover principles, concepts and technological aspects, as well as the procedures followed by the regulatory body for assessing applications for authorization, for inspecting facilities and activities, and for enforcing regulatory requirements.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
119	4	Requirement 20: Liaison with advisory bodies and support organizations	The regulatory body shall obtain technical or other expert professional advice or services as necessary in support of its regulatory functions, but this shall not relieve the regulatory body of its assigned responsibilities.	4.18. The regulatory body may decide to give formal status to the processes by which it is provided with expert opinion and advice. If the establishment of advisory bodies, whether on a temporary or a permanent basis, is considered necessary, it is essential that such bodies provide independent advice, whether technical or non-technical in nature. 4.19. Technical and other expert professional advice or services may be provided in several ways by experts external to the regulatory body. The regulatory body may decide to establish a dedicated support organization, in which case clear limits shall be set for the degree of control and direction by the regulatory body over the work of the support organization. Other forms of external support would require a formal contract between the regulatory body and the provider of advice or services. 4.20. Arrangements shall be made to ensure that there is no conflict of interest for those organizations that provide the regulatory body with advice or services.9 If this is not possible domestically, then the necessary advice or assistance shall be sought from organizations in other States or, as and where appropriate, from international organizations which have no such conflicts of interest. 4.21. If the necessary advice or assistance can be obtained only from organizations whose interests potentially conflict with those of the regulatory body, the seeking of this advice or assistance shall be monitored, and the advice given shall be carefully assessed for conflicts of interest. 4.22. The obtaining of advice and assistance does not relieve the regulatory body of its assigned responsibilities. The regulatory body shall have adequate core competence to make informed decisions. In making decisions, the regulatory body shall have the necessary means to assess advice provided by advisory bodies and information submitted by authorized parties and applicants.		
122	4	Requirement 23: Authorization of facilities and activities by the regulatory body	Authorization by the regulatory body, including specification of the conditions necessary for safety, shall be a prerequisite for all those facilities and activities that are not either explicitly exempted or approved by means of a notification process.			

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
136	5	Principle 1: Responsibility for safety	The prime responsibility for safety must rest with the person or organization responsible for facilities and activities that give rise to radiation risks.	3.3. The person or organization responsible for any facility or activity that gives rise to radiation risks or for carrying out a programme of actions to reduce radiation exposure has the prime responsibility for safety. 3.4. Authorization to operate a facility or conduct an activity may be granted to an operating organization or to an individual, known as the licensee. 3.5. The licensee retains the prime responsibility for safety throughout the lifetime of facilities and activities, and this responsibility cannot be delegated. Other groups, such as designers, manufacturers and constructors, employers, contractors, and consignors and carriers, also have legal, professional or functional responsibilities with regard to safety. 3.6. The licensee is responsible for: —Establishing and maintaining the necessary competences; —Providing adequate training and information; —Establishing procedures and arrangements to maintain safety under all conditions; —Verifying appropriate design and the adequate quality of facilities and activities and of their associated equipment; —Ensuring the safe control of all radioactive material that is used, produced, stored or transported; —Ensuring the safe control of all radioactive waste that is generated. These responsibilities are to be fulfilled in accordance with applicable safety objectives and requirements as established or approved by the regulatory body, and their fulfilment is to be ensured through the implementation of the management system. 3.7. Since radioactive waste management can span many human generations, consideration must be given to the fulfilment of the licensee's (and regulator's) responsibilities in relation to present and likely future operations. Provision must also be made for the continuity of responsibilities and the fulfilment of funding requirements in the long term.	Lack of clear assignment of responsibility for safety Licensee does not assume responsibility for all areas necessary to achieve compliance with safety objectives Lack of consideration for impacts to future generations	Clear definition of prime responsibility for safety Responsibility of licensee covers all areas necessary to achieve compliance with safety objectives Responsibility of licensee includes consideration of imacts on future generations

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
137	5	Principle 2: Role of government	An effective legal and governmental framework for safety, including an independent regulatory body, must be established and sustained.	3.8. A properly established legal and governmental framework provides for the regulation of facilities and activities that give rise to radiation risks and for the clear assignment of responsibilities. The government is responsible for the adoption within its national legal system of such legislation, regulations, and other standards and measures as may be necessary to fulfil all its national responsibilities and international obligations effectively, and for the establishment of an independent regulatory body. 3.9. Government authorities have to ensure that arrangements are made for preparing programmes of actions to reduce radiation risks, including actions in emergencies, for monitoring releases of radioactive substances to the environment and for disposing of radioactive waste. Government authorities have to provide for control over sources of radiation for which no other organization has responsibility, such as some natural sources, 'orphan sources' and radioactive residues from some past facilities and activities. 3.10. The regulatory body must: —Have adequate legal authority, technical and managerial competence, and human and financial resources to fulfil its responsibilities; -Be effectively independent of the licensee and of any other body, so that it is free from any undue pressure from interested parties; —Set up appropriate means of informing parties in the vicinity, the public and other interested parties, and the information media about the safety aspects (including health and environmental aspects) of facilities and activities and about regulatory processes; —Consult parties in the vicinity, the public and other interested parties, as appropriate, in an open and inclusive process. Governments and regulatory bodies thus have an important responsibility in establishing standards and establishing the regulatory framework for protecting people and the environment against radiation risks. However, the prime responsibility for safety rests with the licensee. 3.11. In the event that the licensee is a branch of government, this branch must be clearly identified as distinct from and effectively independent of the branches of government with responsibilities for regulatory functions.	Inadequate legal and regulatory framework Inadequate oversight by regulatory authority Inadequate competence of the regulatory authority Inadequate independence of regulatory authority from licensee	Effective legal and regulatory framework that reflects industry best practice necessary to achieve nuclear safety Effective regulatory responsibilities in place to achieve effective oversight of all licensees necessary to ensure compliance with legal and regulatory requirements Competent staff in the regulatory organization Adequate independence between the regulator and the licensee

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
147	6	3.1.2. Responsibility of the operating organization	Principle: The ultimate responsibility for the safety of a nuclear power plant rests with the operating organization. This is in no way diluted by the separate activities and responsibilities of designers, suppliers, contractors, constructors and regulators.	36. Once the operating organization accepts possession, it is in complete charge of the plant, with full responsibility and commensurate authority for approved activities in the production of electric power. Since these activities also affect the safety of the plant, the operating organization establishes policy for adherence to safety requirements, establishes procedures for safe control of the plant under all conditions, including maintenance and surveillance, and retains a competent, fit and fully trained staff. The operating organization ensures that responsibilities are well defined and documented and that the resources and facilities for the tasks of its staff are in place. 37. The operating organization also has responsibilities in certain areas where its control is less direct, such as with contractors. By using its own staff and resources, or through agencies acting on its behalf, the operating organization institutes rigorous reviews, audits and, as necessary, approval processes to ensure that the factors which determine the safety of the plant are given the necessary attention. This applies, for example, to site investigation, design, manufacturing, construction, testing and commissioning. 38. This principle of the operating organization's overriding safety responsibility is a prime one. The responsibilities of other parties are also significant for safety as well as for financial and legal matters. Variations in national practices make it difficult to define the formal responsibilities of the other parties, but clearly designers, manufacturers and constructors are required as a minimum to provide a sound design and equipment that meets its specifications in terms of both engineering detail and performance of the intended function, meeting or exceeding quality standards commensurate with the safety significance of components or systems. The technical societies and the scientific community generally carry responsibilities for high standards of performance of individuals in the professional sense, and for maintaining and strengthening the basis on which the safety of nuclear power plants stands. The responsibilities of the regulators are discussed in Section 3.1.3.	Lack of clear assignment of responsibility for safety during the operations and maintenance phase of the plant Licensee does not assume responsibility for all areas necessary to achieve and maintain compliance with safety objectives	During the operation and maintenance phase, the operating organization has the overriding responsibility for safety Responsibility for safety is in no way diluted by activities and responsibilities of designers, suppliers, constructors or regulators

156	6	3.3.5. Human factors	Principle: Personnel engaged in activities bearing on nuclear plant safety are trained and qualified to perform their duties. The possibility of human error in nuclear power plant operation is taken into account by facilitating correct decisions by operators and inhibiting wrong decisions, and by providing means for detecting and correcting or compensating for error.	90. One of the most important lessons of abnormal events, ranging from minor incidents to serious accidents, is that they have so often been the result of incorrect human actions. Frequently such events have occurred when plant personnel did not recognize the safety significance of their actions, when they violated procedures, when they were unaware of conditions in the plant, were misled by incomplete data or an incorrect mindset, or did not fully understand the plant in their charge. The operating organization must recognize the high technology aspect of nuclear power plants and must ensure that its staff is able to manage it satisfactorily. 91. The human error component of events and accidents has been too great in the past. The remedy is a twofold approach, through design, including automation, and through improved human performance, including the need to identify expected behaviours, to conduct pre-task reviews, to identify error-likely conditions and to discuss outcomes and responses. In unusual circumstances, optimal use of human ingenuity is required. 92. Engineered features and administrative controls protect against violations of safety provisions. Moreover, attention to human factors at the design stage ensures that plants are tolerant of human error. This is achieved, for example, through the actuation of automatic control or protection systems if operator action causes a plant parameter to exceed normal operational limits or safety system trip points. Designs of protection systems ensure that operator intervention to correct faults is required only in cases where there is sufficient time for diagnosis and corrective action. The control room layout provides for localization and concentration of data and controls used in safety related operations and in accident management. Diagnostic aids are provided to assist in the speedy resolution of safety questions. The data available in the control room are generally sufficient for the diagnosis of any faults that may develop and for assessing the effects of any actions taken. Reliable communication exists between the control room and operating personnel at remote locations who may be required to take action affecting the state of the plant. Administrative measures ensure that such actions by operators at remote locations are properly cleared with the control room staff. The layout and identification of remotely located controls is such as to reduce the chance of error in their selection. 93. ‘Human factor improvements’ are being made in plant hardware (e.g. in ergonomic layout), plant procedures, training and other areas to help prevent or mitigate human error. The objective is to simplify the information reaching the operating personnel and to enable control room personnel to have a clear understanding and control of the status of the plant. In operating plants, task analysis is employed as a technique to review operator and maintenance activities and to determine whether they can be improved by changing the work, the instructions or the procedures. Also, the input of experienced plant operators is sought to simplify the information flow, the control room functions and the process of operation. When replacement control and instrumentation equipment can no longer be purchased, it is replaced when possible by programmable controllers or ‘minicomputer’ systems which augment plant diagnostics. If the software of such controllers and minicomputers is important to safety, the computer software will be designed, implemented and tested according to structured software engineering principles and will include appropriate verification	Personnel involved in safety related activities do not have the competencies to perform the activity adequately Human error is not taken into account in the design of safety related business processes	Personnel involved with safety related activities have the competencies necessary to perform their duties Possibility of human error is taken into account

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				and validation. Additional quality assurance measures are necessary when it is changed by maintenance, including a clear definition of access rights and the assurance of adequate knowledge on the part of maintenance staff. For future nuclear power plants, the opportunities for human factor improvements will be much greater in that the layout and structure of the plants are not yet fixed. Also, digital computer systems are being introduced for safety functions and to substitute self-testing for operator testing. Such computer systems need to be designed and installed to ensure that residual faults and design errors do not prevent any required safety action. 94. To keep the plant within the boundaries of a domain of safe operation, approved procedures for operation are followed. To ensure this, staff training and retraining receive strong emphasis, with classroom, simulator and plant based studies. Operation, maintenance and inspection aids are developed that take account of the strengths and weaknesses of human performance. 95. The foregoing discussion emphasizes the human factor in operation. This is especially important, but attention to this aspect must not lead to neglect of the human factor in maintenance and inspection. Errors in these activities have been important causes of component and system failures in the past. For this reason the procedures ensuring excellence in the performance of operating staff are also followed for maintenance staff.		
196	6	4.5.1. Organization, responsibilities and staffing	Principle: The operating organization exerts full responsibility for the safe operation of a nuclear power plant through a strong organizational structure under the line authority of the plant manager. The plant manager ensures that all elements for safe plant operation are in place, including an adequate number of qualified and experienced personnel.	266. Day to day responsibility for plant safety resides with the plant manager, who ensures that the necessary elements for achieving safety are present and that the need for safety governs operations at the plant. The plant manager is supported by the executive management of the operating organization, which assigns adequate financial and technical support, material, chemistry, radiological protection and other staff resources to the operation. Safety responsibilities for all levels and functions of the operating organization are clearly stated in job descriptions. 267. Enough qualified staff are employed to carry out all normal activities without undue stress or delay, including the supervision of work done by external contractors during periods of exceptional workload such as maintenance outages. Staffing specifications also ensure backup for key positions and take account of attrition and the time required for retraining. 268. Staffing requirements for abnormal operational occurrences are analysed to ensure the capability of carrying out any specialized tasks, such as accident management, damage assessment and control, fire-fighting, search and rescue, first aid treatment, off-site monitoring and off-site communications. These staffing requirements take into account the availability of emergency services in the locality.	Lack of clear assignment of responsibility for safety during the operations and maintenance phase of the plant	Day to day responsibility for safety resides with the plant manager

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
198	6	4.5.3. Conduct of operations	Principle: Operation of the plant is conducted by authorized personnel, according to strict administrative controls and observing procedural discipline.	273. The plant is operated only by suitably trained and qualified staff, who consistently demonstrate in their activities the promotion of safe and reliable operation. They are aware of the significance for safety of their activities and of the consequences for safety of errors. Plant operations are carried out in an environment conducive to safety with staff discipline, the avoidance of inappropriate work patterns and attention to good housekeeping. Managers and supervisors reinforce desired behaviour and practices. The operators on duty monitor the status of the plant on a continuous basis to confirm that components and systems are performing satisfactorily or are in an appropriate state of readiness. They ensure that plant deficiencies and departures from required conditions or plant configurations are detected, and that prompt remedial action is taken. Warning alarms are investigated and required action taken. Unusual phenomena are investigated (such as noise or apparent changes in process or core performance) and appropriate action is taken if there is a danger to vital components or an unexplained response to controls of process or safety systems. Control room and plant routines include observing checklists, recording pertinent plant data, keeping up to date operating logs, passing on data and instructions in shift turnover, and regular walk-down of the plant during shift operations. Particular attention is paid to monitoring when the plant status is changed. 274. The plant is operated on the basis of a hierarchy of approved procedures subject to strict document control. Deviation from these procedures requires approval at a level appropriate to the significance of the changes for safety. Written procedures are kept current. Maintenance and surveillance of plant components and systems are subject to strong control, and maintenance activities are approved by authorized personnel. Plant modifications important for safety are pursued only under approved procedures. Plant configuration is maintained within the intent of the design and safety analysis by adherence to procedures that include strict reporting arrangements for changes in configuration and reviews at appropriate intervals. Plant drawings and descriptions are kept up to date. 275. A formal communication system exists for the transmission of orders and for the transfer of information related to the reliable and safe operation of the plant. This system includes reliable and retrievable recording of instructions and information of possible importance, and of the fact that instructions and orders were received and understood. 276. Measures are enforced that ensure that operating and maintenance staff on duty are alert and mentally unimpaired. If any such personnel are found to be under the influence of alcohol or of consciousness altering drugs, disciplinary action is taken. Further alcohol or drug abuse is grounds for dismissal from positions of responsibility. 277. Special attention is given to physical features and administrative procedures to prevent unauthorized actions, whether intentional or unintentional, by plant personnel or others, that could jeopardize safety.	Personnel involved in safety related activities do not have the competencies to perform the activity adequately in accordance with approved procedures	Operation and maintenance staff are trained and qualified to perform their duties in accordance with approved procedures

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
204	6	4.5.9. Engineering and technical support of operations	Principle: Engineering and technical support, competent in all disciplines important for safety, is available throughout the lifetime of the plant.	297. The continuing safe operation of a nuclear power plant requires the support of an engineering organization, which can be called on as required to assist with plant modifications, repairs and special tests, and to provide analytical support as necessary for the safety of the plant. This resource may be provided within the operating organization itself, or it may be available from the plant suppliers or specialist groups. It is the responsibility of the operating organization to ensure that the resources required are available. 298. Issues relating to the continued availability of knowledgeable and competent engineers in the nuclear power industry are addressed. These include the potential loss of staff owing to competition for engineering expertise from other industrial sectors and the need to consider the effects of staff reductions and loss of expertise as a result of retirement and the closure of nuclear power plants. These factors all lead to the loss of key and experienced personnel and their knowledge about the nuclear industry. As noted under para. 121, it is important to define the necessary complement of core skills to ensure safety and to preserve it over the years.	Engineering and technical support personnel involved in safety related activities do not have the competencies to perform the activity adequately	Engineering and technical support staff are competent to perform tasks assigned to them
209	6	4.6.2. Training and procedures for accident management	Principle: Nuclear plant staff are trained and retrained in the procedures to follow if an accident occurs that exceeds the design basis of the plant.	324. The members of the operating staff are made familiar with the features of the analysis described in the principle in Section 4.6.1 as part of their training programme. The procedures used for accident management are the plant emergency operating procedures, including those parts dealing with ultimate emergencies. Ultimate emergency procedures are general in nature and serve to remind the operators of the capabilities of the plant for mitigating the course and consequences of severe accidents. The ultimate procedures are also flexible so that they can be adjusted to the uncertainties of more extreme accidents. Training and testing of plant operators ensure their familiarity with the symptoms of accidents beyond the design basis and the procedures for accident management. Simulators are indispensable training tools. However, they must be able to represent correctly the way in which an accident would evolve, at least up to the occurrence of extensive fuel damage. Personnel assignments are defined for a specialist team to advise operators in the event of an accident that exceeds the design basis. This team includes personnel who are familiar with the severe accident analysis for the plant. 325. Since existing training simulators do not tend to simulate severe core damage, the training for severe accidents concentrates on plant walk throughs, classes on the associated phenomena and the strategies and/or guidance proposed for dealing with their hazards and risks.	Personnel involved in accident management activities do not have the competencies to perform the activity adequately	Staff are trained in procedures to follow if an accident occurs that exceeds the design basis of the plant

OPERATIONS AND MAINTENANCE PHASE

Governance

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
73	2	Requirement 1: Responsibilities of the operating organization	The operating organization shall have the prime responsibility for safety in the operation of a nuclear power plant.	3.1. The prime responsibility for safety shall be assigned to the operating organization of the nuclear power plant. This prime responsibility shall cover all the activities relating to the operation directly and indirectly. It includes the responsibility for supervising the activities of all other related groups, such as designers, suppliers, manufacturers and constructors, employers and contractors, as well as the responsibility for operation of nuclear power plant(s) by the operating organization itself. The operating organization shall discharge this responsibility in accordance with its management system [3]. components for establishing policies and objectives and enabling the objectives to be achieved in an efficient and effective manner, shall include the following activities: (a) Policy making for all areas of safety, which includes: —Setting management objectives; —Establishing the policy for safety; —Developing management and staff who value learning, have skills in creating, acquiring and transferring knowledge, and can adapt the organization on the basis of new knowledge and insights; —Promoting a strong safety culture. Strategies and management objectives shall be developed in accordance with the policy in order to put the policy into effect. (b) Allocation of responsibilities with corresponding lines of authority and communication, for: —Allocating resources; —Providing human resources with the appropriate level of education and training and material resources; —Retaining the necessary competences; —Approving the contents of management programmes; —Developing procedures and instructions, and having a strict policy of adherence to these procedures and instructions; —Setting policies on fitness for duty; —Establishing a programme to make the necessary changes to any of these functions on the basis of the performance in achieving objectives. (c) Operating functions, which include executive decision making and actions for the operation of a plant for all operational states and accident conditions. (d) Support activities, which include obtaining, from both on-site and off-site organizations, including contractors, the technical and administrative services and the use of facilities necessary to perform the operating functions. For sites with shared safety related resources (e.g. sites with multiple units or with more than one operating organization), the arrangements for the use of such shared resources shall be clearly defined. (e) Review activities, which include monitoring and assessing the performance of the operating functions and supporting functions on a regular basis. The purpose of monitoring is: to verify compliance with the objectives for safe operation of the plant; to reveal deviations, deficiencies and equipment failures; and to provide information for the purpose of taking timely corrective actions and making improvements. Reviewing functions shall also include review of the overall safety performance of the organization to assess the effectiveness of management for safety and to identify opportunities for improvement. In addition, a safety review of the plant shall be performed periodically, including design aspects, to ensure that the plant is operated in conformance with the approved design and safety analysis report, and to identify possible safety improvements. (f) Design integrity, which includes maintaining a formally designated entity that has overall responsibility for the continuing integrity of the plant design throughout its lifetime, and managing the interfaces and lines of communication with the responsible designers and equipment suppliers contributing to this continuing integrity [2]. 3.3. The operating organization shall establish liaison with the regulatory body and with relevant authorities to ensure a common understanding of, and to ensure compliance with, safety requirements and their interface with other requirements, such as those for security, protection of health or protection of the environment.	Responsibility for some safety related activities is not undertaken by anyone.	Safety management system Clear responsibility for overall responsibility of design integrity Management of responsibilities and interfaces between safety related activities, especially when involving off-site organizations and contractors. Clear policies and governance defining responsibilities for safety related activities Personnel development program that ensures personnel have the necessary competencies to perform safety related activities assigned to them Review, monitoring and assessment of safety related activities on a regular basis

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
74	2	Requirement 5: Safety policy	The operating organization shall establish and implement operational policies that give safety the highest priority.	4.1. The operational policy established and implemented by the operating organization shall give safety the utmost priority, overriding the demands of production and project schedules. The safety policy shall promote a strong safety culture, including a questioning attitude and a commitment to excellent performance in all activities important to safety. Managers shall promote an attitude of safety consciousness among plant staff [3]. 4.2. The safety policy shall stipulate clearly the leadership role of the highest level of management in safety matters. Senior management shall communicate the provisions of the safety policy throughout the organization. Safety performance standards shall be developed for all operational activities and shall be applied by all site personnel. All personnel in the organization shall be made aware of the safety policy and of their responsibilities for ensuring safety. The safety performance standards and the expectations of the management for safety performance shall be clearly communicated to all personnel, and it shall be ensured that they are understood by all those involved in their implementation. 4.3. Key aspects of the safety policy shall be communicated to external support organizations, including contractors, so that the operating organization's requirements and expectations for the safety related activities of external support organizations, including contractors, will be understood and met. 4.4. The safety policy of the operating organization shall include commitments to perform periodic safety reviews of the plant throughout its operating lifetime in compliance with the regulatory requirements. Operating experience and significant new safety related information from relevant sources, including information on agreed corrective actions and on necessary improvements that have been implemented, shall be taken into account (see also Requirement 12). 4.5. The safety policy of the operating organization shall include a commitment to achieving enhancements in operational safety. The strategy of the operating organization for enhancing safety and for finding more effective ways of applying and, where feasible, improving existing standards shall be continuously monitored and supported by means of a clearly specified programme with clear objectives and targets.	Demands of production or project schedules overrode safety related considerations Personnel were unaware of the safety policies or did not understand them Personnel ignored safety policies Lack of safety reviews that take into account operating experience from both within and outside the organization Lack of a program to continually improve operational safety	Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety Safety policies establishing the priority for safety and the standards to be met for all safety related activities Programs to communicate and train personnel in the safety policies Continuous improvement program focused on operational safety Periodic safety review program including review of operational experience inside and outside the organization

75	2	Requirement 6: Operational limits and conditions	The operating organization shall ensure that the plant is operated in accordance with the set of operational limits and conditions.	4.6. The operational limits and conditions shall form an important part of the basis for the authorization of the operating organization to operate the plant. The plant shall be operated within the operational limits and conditions to prevent situations arising that could lead to anticipated operational occurrences or accident conditions, and to mitigate the consequences of such events if they do occur. The operational limits and conditions shall be developed for ensuring that the plant is being operated in accordance with the design assumptions and intent, as well as in accordance with its licence conditions. 4.7. The operational limits and conditions shall reflect the provisions made in the final design as described in the safety analysis report. The operational limits and conditions shall be submitted to the regulatory body for assessment and approval before the commencement of operation, if so required by the regulatory body. All operational limits and conditions shall be substantiated by a written statement of the reason for their adoption. 4.8. The operational limits and conditions shall be reviewed and revised as necessary in consideration of experience, developments in technology and approaches to safety, and changes in the plant. 4.9. The operational limits and conditions shall include requirements for normal operation, including shutdown and outage stages, and shall cover actions to be taken and limitations to be observed by the operating personnel. 4.10. The operational limits and conditions shall include the following: (a) Safety limits; (b) Limiting settings for safety systems; (c) Limits and conditions for normal operation; (d) Surveillance and testing requirements; (e) Action statements for deviations from normal operation. 4.11. Operating personnel who are directly responsible for the conduct of operations shall be trained in and shall be thoroughly familiar with the operational limits and conditions in order to comply with the provisions contained therein. 4.12. The operating organization shall ensure that an appropriate surveillance programme is established and implemented to ensure compliance with the operational limits and conditions, and that its results are evaluated, recorded and retained. 4.13. The plant shall be returned to a safe operational state when an event occurs in which parameters deviate from the limits and conditions for normal operation. Appropriate remedial actions shall be taken. The operating organization shall undertake a review and evaluation of the event. The regulatory body shall be notified in accordance with the established event reporting system. 4.14. A process shall be established to ensure that deviations from operational limits and conditions are documented and reported in an appropriate manner and	Operating limits and conditions are not well documented, and/or do not cover all necessary limits and conditions Operating limits and conditions are not consistent with design assumptions and intent Operating limits and conditions were not revised to take into account operating experience Personnel responsible for conduct of safety related activiites did not have a complete understanding of the operating limits and conditions Deviations from operating limits and conditions were not detected and/or appropriate remedial actions were not taken	A complete set of operating limits and conditions are documented and consistent with design assumptions and intent A continuous improvement program is established that revises operating limits and conditions based on operating experience A monitoring and surveillance program is established that detects deviations from operating limits and conditions, and takes appropriate remedial actions A training program is established to ensure that personnel assigned safety related activities are knowledgeable of the operating limits and conditions

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				that appropriate actions are taken in response. Responsibilities and lines of communication for responding to such deviations shall be clearly specified in writing. 4.15. The operating organization shall not intentionally exceed the operational limits and conditions. Where circumstances necessitate plant operation outside the operational limits and conditions, clear formal instructions for such operations shall be developed, on the basis of safety analysis, if applicable. These instructions shall include instructions for returning the plant to normal operation within the operational limits and conditions. The instructions shall also include specification of the arrangements for approval by the operating organization and the regulatory body, as appropriate, of the changed operational limits and conditions, prior to operation under these changed operational limits and conditions.		
65	3	Requirement 12: Fostering a culture for safety	Individuals in the organization, from senior managers downwards, shall foster a strong safety culture. The management system and leadership for safety shall be such as to foster and sustain a strong safety culture.	5.1. All individuals in the organization shall contribute to fostering and sustaining a strong safety culture [1, 2]. 5.2. Senior managers and all other managers shall advocate and support the following: (a) A common understanding of safety and of safety culture, including: awareness of radiation risks and hazards relating to work and to the working environment; an understanding of the significance of radiation risks and hazards for safety; and a collective commitment to safety by teams and individuals; (b) Acceptance by individuals of personal accountability for their attitudes and conduct with regard to safety; (c) An organizational culture that supports and encourages trust, collaboration, consultation and communication; (d) The reporting of problems relating to technical, human and organizational factors and reporting of any deficiencies in structures, systems and components to avoid degradation of safety, including the timely acknowledgement of, and reporting back of, actions taken; (e) Measures to encourage a questioning and learning attitude at all levels in the organization and to discourage complacency with regard to safety; (f) The means by which the organization seeks to enhance safety and to foster and sustain a strong safety culture, and using a systemic approach (i.e. an approach relating to the system as a whole in which the interactions between technical, human and organizational factors are duly considered); (g) Safety oriented decision making in all activities; (h) The exchange of ideas between, and the combination of, safety culture and security culture.	Lack of a strong safety culture Lack of understanding by personnel of safety and safety culture Lack of commitment of personnel to their role in achieving safety Lack of trust and effective communications with respect to raising issues with respect to safety Lack of taking safety into account in all decision making	Clearly defined responsibilities for all managers to advocate and support a safety culture Programs to educate personnel their role in achieving and maintaining safety Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety Safety policies establishing the priority for safety and the standards to be met for all safety related activities

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
66	3	Requirement 2: Demonstration of leadership for safety by managers	Managers shall demonstrate leadership for safety and commitment to safety.	3.1. The senior management of the organization shall demonstrate leadership for safety by: (a) Establishing, advocating and adhering to an organizational approach to safety that stipulates that, as an overriding priority, issues relating to protection and safety receive the attention warranted by their significance; (b) Acknowledging that safety encompasses interactions between people, technology and the organization [2]; (c) Establishing behavioural expectations and fostering a strong safety culture; (d) Establishing the acceptance of personal accountability in relation to safety on the part of all individuals in the organization and establishing that decisions taken at all levels take account of the priorities and accountabilities for safety. 3.2. Managers at all levels in the organization, taking into account their duties, shall ensure that their leadership includes: (a) Setting goals for safety that are consistent with the organization's policy for safety, actively seeking information on safety performance within their area of responsibility and demonstrating commitment to improving safety performance; (b) Development of individual and institutional values and expectations for safety throughout the organization by means of their decisions, statements and actions; (c) Ensuring that their actions serve to encourage the reporting of safety related problems, to develop questioning and learning attitudes, and to correct acts or conditions that are adverse to safety. 3.3. Managers at all levels in the organization: (a) Shall encourage and support all individuals in achieving safety goals and performing their tasks safely; (b) Shall engage all individuals in enhancing safety performance; (c) Shall communicate clearly the basis for decisions relevant to safety.	Lack of a strong safety culture Lack of understanding by personnel of safety and safety culture Lack of commitment of personnel to their role in achieving safety Lack of trust and effective communications with respect to raising issues with respect to safety Lack of taking safety into account in all decision making	Clearly defined responsibilities for all managers to advocate and support a safety culture Programs to educate personnel their role in achieving and maintaining safety Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety Safety policies establishing the priority for safety and the standards to be met for all safety related activities
67	3	Requirement 3: Responsibility of senior management for the management system	Senior management shall be responsible for establishing, applying, sustaining and continuously improving a management system to ensure safety.	4.1. Senior management shall retain accountability for the management system even where individuals are assigned responsibility for coordinating the development, application and maintenance of the management system [1, 2]. 4.2. Senior management shall be responsible for establishing safety policy.	Lack of an effective safety management system	Clear definition of the accountabilty of senior managers for establishing an effective safety management system

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
68	3	Requirement 4: Goals, strategies, plans and objectives	Senior management shall establish goals, strategies, plans and objectives for the organization that are consistent with the organization's safety policy.	4.3. Goals, strategies, plans and objectives for the organization shall be developed in such a manner that safety is not compromised by other priorities. 4.4. Senior management shall ensure that measurable safety goals that are in line with these strategies, plans and objectives are established at various levels in the organization. 4.5. Senior management shall ensure that goals, strategies and plans are periodically reviewed against the safety objectives, and that actions are taken where necessary to address any deviations.	Safety is not given sufficient priority when establishing goals, strategies, plans and objectives for the organization The safety management system is not effective at measuring progress in achieving goals, strategies, plans and objectives and not effective at taking actions to deal with deviations	Establishment of a safety management system that establishes safety goals, strategies, plans and objectives including their measurement and review to identify necessary actions to deal with deviations
70	3	Requirement 6: Integration of the management system	The management system shall integrate its elements, including safety, health, environmental, security, quality, human-and-organizational-factor, societal and economic elements, so that safety is not compromised.	4.8. The management system shall be developed, applied and continuously improved. It shall be aligned with the safety goals of the organization. 4.9. The management system shall be applied to achieve goals safely, to enhance safety and to foster a strong safety culture by: (a) Bringing together in a coherent manner all the necessary elements for safely managing the organization and its activities; (b) Describing the arrangements made for management of the organization and its activities; (c) Describing the planned and systematic actions necessary to provide confidence that all requirements are met; (d) Ensuring that safety is taken into account in decision making and is not compromised by any decisions taken. 4.10. Arrangements shall be made in the management system for the resolution of conflicts arising in decision making processes. Potential impacts of security measures on safety and potential impacts of safety measures on security shall be identified and shall be resolved without compromising safety or security [20–23]. 4.11. The organizational structures, processes, responsibilities, accountabilities, levels of authority and interfaces within the organization and with external organizations shall be clearly specified in the management system. 4.12. Regulatory requirements shall be reflected in the management system. 4.13. Provision shall be made in the management system to identify any changes (including organizational changes and the cumulative effects of minor changes) that could have significant implications for safety and to ensure that they are appropriately analysed. 4.14. Arrangements shall be established in the management system for an independent review to be made before decisions significant for safety are made. The requirements on the independent nature of the review and on the necessary competences of the reviewers shall be specified in the management system.	Lack of alignment of the management system with the safety goals of the organizations Lack of safe resolution of conflicts arising in decision making Unclear safety related organizational structures, processes, responsibilities, accountabilities, levels of authority, and interfaces within the organization and with external organizations. The cumulative effect of minor changes to the plant, processes and organization result in significant implications for safety.	Establishment of a safety management system that establishes safety goals, strategies, plans and objectives including their measurement and review to identify necessary actions to deal with deviations Integration of the safety management system into the management system of the organizations

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
72	3	Requirement 8: Documentation of the management system	The management system shall be documented. The documentation of the management system shall be controlled, usable, readable, clearly identified and readily available at the point of use.	4.16. The documentation of the management system shall include as a minimum: policy statements of the organization on values and behavioural expectations; the fundamental safety objective; a description of the organization and its structure; a description of the responsibilities and accountabilities; the levels of authority, including all interactions of those managing, performing and assessing work and including all processes; a description of how the management system complies with regulatory requirements that apply to the organization; and a description of the interactions with external organizations and with interested parties. 4.17. Documents shall be controlled. All individuals responsible for preparing, reviewing, revising and approving documents shall be competent to perform the tasks and shall be given access to appropriate information on which to base their input or decisions. 4.18. Revisions to documents shall be controlled, reviewed and recorded. Revised documents shall be subject to the same level of approval as the initial documents. 4.19. Records shall be specified in the management system and shall be controlled. All records shall be readable, complete, identifiable and easily retrievable. 4.20. Retention times of records and associated test materials and specimens shall be established to be consistent with the statutory requirements and with the obligations for knowledge management of the organization. The media used for records shall be such as to ensure that the records are readable for the duration of the retention times specified for each record.	Poor safety related decisions	Establishment of a safety management system that is clearly documented Establishment of a document and records management system so that all safety related documents are controlled and the correct version of documents and records are available to personnel requiring them

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
76	3	Requirement 1: Achieving the fundamental safety objective	The registrant or licensee — starting with the senior management — shall ensure that the fundamental safety objective of protecting people and the environment from harmful effects of ionizing radiation is achieved.	2.1. The registrant or licensee shall ensure that provisions are made to achieve the fundamental safety objective. 2.2. The senior management of organizations, in accordance with their accountabilities: (a) Shall ensure the safe siting, design, construction, commissioning, operation and decommissioning (or closure) of facilities [2, 9, 11–14]; (b) Shall ensure that equipment and activities meet safety standards, quality standards and management standards; (c) Shall ensure the safe management and control of all radioactive material and radiation sources that are produced, processed, used, handled, transported, stored or disposed of [5, 15]; (d) Shall ensure that managers at all levels in the organization develop and maintain an understanding of radiation risks and potential consequences, and of how to manage radiation risks relevant to their responsibilities [16]; (e) Shall ensure that provision is made for adequate resources and funding, including for the long term management and disposal of radioactive waste, as well as for decommissioning (or closure) of facilities, with due consideration given to the protection of future generations [9, 15, 17]; (f) Shall ensure that adequate arrangements are made where appropriate for preparedness and response for a nuclear or radiological emergency [18, 19].	Safety related equipment and activities do not satisfy standards for safety, quality and management. Lack of understanding by managers of radiation risks and how to manage them Lack of adequate resources and funding for achieving and maintaining safety including during decommissioning and radioactive waster disposal. Lack of adequate arrangements for responding to a nuclear or radiological emergency	Clear definition of accountabilities for managers responsible for the safety of the plant during siting, design, construction, commissioning, operation and decommissioning. Establishing processes, organizations and governance in compliance with standards for safety, quality and management. Establishing governance that ensures adequate resources and funding are available to achieve and maintain safety including during decommissioning and for radioactive waste disposal Establishment of an adequate emergency preparedness program.
100	4	Requirement 1: National policy and strategy for safety	The government shall establish a national policy and strategy for safety, the implementation of which shall be subject to a graded approach in accordance with national circumstances and with the radiation risks associated with facilities and activities, to achieve the fundamental safety objective and to apply the fundamental safety principles established in the Safety Fundamentals.	2.3. National policy and strategy for safety shall express a long term commitment to safety. The national policy shall be promulgated as a statement of the government's intent. The strategy shall set out the mechanisms for implementing the national policy. In the national policy and strategy, account shall be taken of the following: (a) The fundamental safety objective and the fundamental safety principles established in the Fundamental Safety Principles [1]; (b) Binding international legal instruments, such as conventions and other relevant international instruments; (c) The specification of the scope of the governmental, legal and regulatory framework for safety; (d) The need and provision for human and financial resources; (e) The provision and framework for research and development; (f) Adequate mechanisms for taking account of social and economic developments; (g) The promotion of leadership and management for safety, including safety culture. 2.4. The national policy and strategy for safety shall be implemented in accordance with a graded approach, depending on national circumstances, to ensure that the radiation risks associated with facilities and activities, including activities involving the use of radiation sources, receive appropriate attention by the government or by the regulatory body.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
101	4	Requirement 2: Establishment of a framework for safety	The government shall establish and maintain an appropriate governmental, legal and regulatory framework for safety within which responsibilities are clearly allocated.	2.5. The government shall promulgate laws and statutes to make provision for an effective governmental, legal and regulatory framework for safety. This framework for safety shall set out the following: (1) The safety principles for protecting people — individually and collectively — society and the environment from radiation risks, both at present and in the future; (2) The types of facilities and activities that are included within the scope of the framework for safety; (3) The type of authorization that is required for the operation of facilities and for the conduct of activities, in accordance with a graded approach; (4) The rationale for the authorization of new facilities and activities, as well as the applicable decision making process; (5) Provision for the involvement of interested parties and for their input to decision making; (6) Provision for assigning legal responsibility for safety to the persons or organizations responsible for the facilities and activities, and for ensuring the continuity of responsibility where activities are carried out by several persons or organizations successively; (7) The establishment of a regulatory body, as addressed in Requirements 3 and 4; (8) Provision for the review and assessment of facilities and activities, in accordance with a graded approach; (9) The authority and responsibility of the regulatory body for promulgating (or preparing for the enactment of) regulations and preparing guidance for their implementation; (10) Provision for the inspection of facilities and activities, and for the enforcement of regulations, in accordance with a graded approach; (11) Provision for appeals against decisions of the regulatory body; (12) Provision for preparedness for, and response to, a nuclear or radiological emergency; (13) Provision for an interface with nuclear security; (14) Provision for an interface with the system of accounting for, and control of, nuclear material; (15) Provision for acquiring and maintaining the necessary competence nationally for ensuring safety; (16) Responsibilities and obligations in respect of financial provision for the management of radioactive waste and of spent fuel, and for decommissioning of facilities and termination of activities; (17) The criteria for release from regulatory control; (18) The specification of offences and the corresponding penalties; (19) Provision for controls on the import and export of nuclear material and radioactive material, as well as for their tracking within, and to the extent possible outside, national boundaries, such as tracking of the authorized export of radioactive sources. 2.6. Where several authorities are involved, the government shall specify clearly the responsibilities and functions of each authority within the governmental, legal and regulatory framework for safety.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
102	4	Requirement 3: Establishment of a regulatory body	The government, through the legal system, shall establish and maintain a regulatory body, and shall confer on it the legal authority and provide it with the competence and the resources necessary to fulfil its statutory obligation for the regulatory control of facilities and activities.			
105	4	Requirement 6: Compliance with regulations and responsibility for safety	The government shall stipulate that compliance with regulations and requirements established or adopted by the regulatory body does not relieve the person or organization responsible for a facility or an activity of its prime responsibility for safety.	2.14. The legal framework for safety shall be established in such a way that the authorized party retains the prime responsibility for safety throughout the lifetime of facilities and the duration of activities, and shall not delegate this prime responsibility. Responsibility for safety may be transferred to a different authorized party when there has been a declared change, approved by the regulatory body, of general responsibility for a facility or activity. In addition, responsibility for safety may extend to other groups associated with the authorized party, such as designers, suppliers, manufacturers and constructors, employers, contractors, and consignors and carriers, in so far as their activities or products may be of significance for safety. However, in no case may this extension of responsibility relieve the authorized party of the prime responsibility for safety. The authorized party has the responsibility for verifying that products and services meet its expectations (e.g. in terms of completeness, validity or robustness) and that they comply with regulatory requirements. 2.15. The prime responsibility for safety shall extend to all stages in the lifetime of facilities and the duration of activities, until their release from regulatory control, i.e. to site evaluation, design, construction, commissioning, operation, shutdown and decommissioning (or closure in the case of disposal facilities for radioactive waste) of facilities. This prime responsibility for safety includes, as appropriate, responsibility for the management of radioactive waste and the management of spent fuel, and responsibility for the remediation of contaminated areas. It also includes responsibility for activities in which radioactive material and radioactive sources are produced, used, stored, transported or handled. 2.15A. The person or organization responsible for a facility or an activity, having prime responsibility for safety, shall actively evaluate progress in science and technology as well as relevant information from the feedback of experience, in order to identify and to make8 those safety improvements that are considered practicable. 2.16. Persons who, or organizations that are responsible for facilities or activities in which radioactive waste is generated shall have responsibility for safety in the management of the radioactive waste, including waste characterization and storage of the radioactive waste [3]. 2.17. For ensuring safety in the transport of radioactive material, reliance is placed primarily on the performance of packages [4]. It is the responsibility of the consignor to ensure the appropriate selection of the package and packaging and the mode of transport.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
107	4	Requirement 8: Emergency preparedness and response	The government shall make provision for emergency preparedness to enable a timely and effective response in a nuclear or radiological emergency.	2.20. The government shall make each authorized party responsible for preparing an emergency plan and for making arrangements for emergency preparedness and response [5]. Emergency arrangements shall include a clear assignment of responsibility for immediate notification of an emergency to the response organizations. The regulatory body shall take account of the fact that, in an emergency, routine regulatory administration such as the issue of prior authorizations may need to be suspended in favour of a timely emergency response. 2.21. In addition to assigning the responsibilities of authorized parties, the government shall establish a nationwide system, including emergency arrangements, to protect the public in a nuclear or radiological emergency declared as a consequence of an incident within or outside the territories and jurisdiction of the State. 2.22. The government shall designate response organizations that will have the responsibilities and resources necessary to make preparations and arrangements for dealing with the consequences of incidents in facilities and activities that affect, or that might affect, the public and the environment. Such preparations shall include planning the actions to be taken both in an emergency and in its aftermath. 2.23. The government shall specify and shall assign clear responsibilities so that timely and effective decisions can be made in an emergency, and shall make provision for effective coordination of and communication between authorized parties and response organizations [5]. 2.24. In preparing an emergency plan and in the event of an emergency, the regulatory body shall advise the government and response organizations, and shall provide expert services (e.g. services for radiation monitoring and risk assessment for actual and expected future radiation risks) in accordance with the responsibilities assigned to it [5]. 2.24A. The government shall ensure that adequate training, drills and exercises, involving authorized parties and response organizations, including decision makers, are carried out regularly to contribute to an effective emergency response [5]. The training, drills and exercises shall cover a full range of postulated emergencies (e.g. events affecting several facilities on the same site, emergency exercises of long duration and emergencies with transboundary consequences). 2.24B. The government shall ensure that arrangements, commensurate with the radiation risks, are in place to inform the general public and members of the public who are affected, or are potentially affected, about measures for emergency preparedness and response. These arrangements shall include arrangements for the provision of information before, during and after operation, until release of the facility or radiation source from regulatory control. Members of the public concerned shall be informed of the potential for a nuclear or radiological emergency, the nature of the associated hazards, the ways in which people will be alerted or notified, and actions to be taken, as appropriate [5].		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
110	4	Requirement 11: Competence for safety	The government shall make provision for building and maintaining the competence of all parties having responsibilities in relation to the safety of facilities and activities.	2.34. As an essential element of the national policy and strategy for safety, the necessary professional training for maintaining the competence of a sufficient number of suitably qualified and experienced staff shall be made available. 2.35. The building of competence shall be required for all parties with responsibilities for the safety of facilities and activities, including authorized parties, the regulatory body and organizations providing services or expert advice on matters relating to safety. Competence shall be built, in the context of the regulatory framework for safety, by such means as: —Technical training; —Learning through academic institutions and other learning centres; —Research and development work. 2.36. The government: (a) Shall stipulate a necessary level of competence for persons with responsibilities in relation to the safety of facilities and activities; (b) Shall make provision for adequate arrangements for the regulatory body and its support organizations to build and maintain expertise in the disciplines necessary for discharge of the regulatory body's responsibilities in relation to safety; (c) Shall make provision for adequate arrangements for increasing, maintaining and regularly verifying the technical competence of persons working for authorized parties. 2.37. In cases where the training programmes available in the State are insufficient, arrangements for training shall be made with other States or with international organizations. 2.38. Development of the necessary competence for the operation and regulatory control of facilities and activities shall be facilitated by the establishment of, or participation in, centres where research and development work and practical applications are carried out in key areas for safety.		
111	4	Requirement 12: Interfaces of safety with nuclear security and with the State system of accounting for, and control of, nuclear material	The government shall ensure that, within the governmental and legal framework, adequate infrastructural arrangements are established for interfaces of safety with arrangements for nuclear security and with the State system of accounting for, and control of, nuclear material.	2.39. Specific responsibilities within the governmental and legal framework shall include: (a) Assessment of the configuration of facilities and activities for the optimization of safety, with factors relating to nuclear security and to the system of accounting for, and control of, nuclear material being taken into account; (b) Oversight and enforcement to maintain arrangements for safety, nuclear security and the system of accounting for, and control of, nuclear material; (c) Liaison with law enforcement agencies, as appropriate; (d) Integration of emergency arrangements for safety related and nuclear security related incidents. 2.40. Safety measures and nuclear security measures shall be designed and implemented in an integrated manner so that nuclear security measures do not compromise safety and safety measures do not compromise nuclear security.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
112	4	Requirement 13: Provision of technical services	The government shall make provision, where necessary, for technical services in relation to safety, such as services for personal dosimetry, environmental monitoring and the calibration of equipment.	2.41. Technical services do not necessarily have to be provided by the government. However, if no suitable commercial or non-governmental provider of the necessary technical services is available, the government may have to make provision for the availability of such services. The regulatory body shall authorize technical services that may have significance for safety, as appropriate.		
118	4	Requirement 19: The management system of the regulatory body	The regulatory body shall establish, implement, and assess and improve a management system that is aligned with its safety goals and contributes to their achievement.	4.14. The regulatory body shall establish and implement a management system whose processes are open and transparent [10]. The management system of the regulatory body shall be continuously assessed and improved. 4.15. The management system of the regulatory body has three purposes: (1) To ensure that the responsibilities assigned to the regulatory body are properly discharged; (2) To maintain and improve the performance of the regulatory body by means of the planning, control and supervision of its safety related activities; (3) To foster and support a safety culture in the regulatory body through the development and reinforcement of leadership as well as good attitudes and behaviour in relation to safety on the part of individuals and teams. 4.16. The management system shall maintain the efficiency and effectiveness of the regulatory body in discharging its responsibilities and performing its functions. This includes the promotion of enhancements in safety, and the fulfilment of its obligations in an appropriate, timely and cost effective manner so as to build confidence. 4.17. The management system shall specify, in a coherent manner, the planned and systematic actions necessary to provide confidence that the statutory obligations placed on the regulatory body are being fulfilled. Furthermore, regulatory requirements shall be considered in conjunction with the more general requirements under the management system of the regulatory body; this helps to prevent safety from being compromised.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
121	4	Requirement 22: Stability and consistency of regulatory control	The regulatory body shall ensure that regulatory control is stable and consistent.	4.26. The regulatory process shall be a formal process that is based on specified policies, principles and associated criteria, and that follows specified procedures as established in the management system. The process shall ensure the stability and consistency of regulatory control and shall prevent subjectivity in decision making by individual staff members of the regulatory body. The regulatory body shall be able to justify its decisions if they are challenged. In connection with its reviews and assessments and its inspections, the regulatory body shall inform applicants of the objectives, principles and associated criteria for safety on which its requirements, judgements and decisions are based. 4.27. The regulatory body shall emphasize the continuous enhancement of safety as a general objective. However, it shall also recognize the risks associated with making modifications to well established practices. Prospective changes in regulatory requirements shall be subject to careful scrutiny, to evaluate the possible enhancements in safety that are to be achieved. The regulatory body shall also inform and consult interested parties in relation to the basis for such proposed changes in regulatory requirements. 4.28. There shall be consistency in the decision making process of the regulatory body and in the regulatory requirements themselves, to build confidence among interested parties.		

123	4	Requirement 24: Demonstration of safety for the authorization of facilities and activities	The applicant shall be required to submit an adequate demonstration of safety in support of an application for the authorization of a facility or an activity.	4.29. Different types of authorization shall be obtained for the different stages in the lifetime of a facility or the duration of an activity. The regulatory body shall be able to modify authorizations for safety related purposes. For a facility, the stages in the lifetime usually include: site evaluation, design, construction, commissioning, operation, shutdown and decommissioning (or closure). This includes, as appropriate, the management of radioactive waste and the management of spent fuel, and the remediation of contaminated areas. For radioactive sources and radiation generators, the regulatory process shall continue over their entire lifetime. 4.30. Authorization for a facility shall include authorization of the activities taking place at the facility (e.g. operation, maintenance and engineering activities). The regulatory body shall verify, by appropriate means, the competence of individuals having responsibilities for the safety of authorized facilities and activities. 4.31. In the granting of an authorization for a facility or an activity, the regulatory body may have to impose limits, conditions and controls on the authorized party's subsequent activities. 4.32. The regulatory body shall establish a process that allows the authorized party to appeal against a regulatory decision relating to an authorization for a facility or an activity or a condition attached to an authorization. 4.33. Prior to the granting of an authorization, the applicant shall be required to submit a safety assessment [9], which shall be reviewed and assessed by the regulatory body in accordance with clearly specified procedures. The extent of the regulatory control applied shall be commensurate with the radiation risks associated with facilities and activities, in accordance with a graded approach. 4.34. The regulatory body shall issue guidance on the format and content of the documents to be submitted by the applicant in support of an application for an authorization. The applicant shall be required to submit or to make available to the regulatory body, in accordance with agreed timelines, all necessary safety related information as specified in advance or as requested in the authorization process. 4.35. Some of the stages in the lifetime of a facility or the duration of an activity (see para. 4.29) may require specific hold points at which separate authorizations are required. In such cases, the completed stages have to be subject to review and assessment, with account taken of feedback from the previous stages. 4.36. An authorization may have to be reconsidered and/or renewed in the different stages in the lifetime of the facility or the duration of the activity concerned (e.g. as a result of a change in the conditions under which the authorization was granted). This would have to lead to a new regulatory decision which may require the amendment, renewal, suspension or revocation of the authorization. 4.37. Any subsequent amendment, renewal, suspension or revocation of the authorization for a facility or an activity shall be undertaken in accordance with a clearly specified and established procedure, and shall make provision for the timely submission of applications for the renewal or amendment of the authorization. 4.38. The safety assessment may need to be repeated or reaffirmed by the regulatory body in support of its decision. The results of regulatory actions such as inspections, reviews and assessments, and feedback from operational

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				performance (e.g. feedback on the exceeding of limits and conditions or on incidents), shall be taken into account in making decisions on the amendment, renewal, suspension or revocation of authorizations. 4.39. The regulatory body shall record formally the basis for its decision on the authorization of a facility or an activity, or on its amendment, renewal, suspension or revocation, and shall inform the applicant, in a timely manner, of its decision, and provide the applicant with reasons and a justification for the decision.		
129	4	Requirement 30: Establishment of an enforcement policy	The regulatory body shall establish and implement an enforcement policy within the legal framework for responding to non-compliance by authorized parties with regulatory requirements or with any conditions specified in the authorization.			
130	4	Requirement 31: Requiring of corrective action by authorized parties	In the event that risks are identified, including risks unforeseen in the authorization process, the regulatory body shall require corrective actions to be taken by authorized parties.	4.54. The response of the regulatory body to non-compliances with regulatory requirements or with any conditions specified in the authorization shall be commensurate with the significance for safety of the non-compliance, in accordance with a graded approach. 4.55. Enforcement actions by the regulatory body may include recorded verbal notification, written notification, imposition of additional regulatory requirements and conditions, written warnings, penalties and, ultimately, revocation of the authorization. Regulatory enforcement may also entail prosecution, especially in cases where the authorized party does not cooperate satisfactorily in the remediation or resolution of the non-compliance. 4.56. At each significant step in the enforcement process, the regulatory body shall identify and document the nature of non-compliances and the period of time allowed for correcting them, and shall communicate this information in writing to the authorized party. 4.57. The authorized party shall be held accountable for remedying non-compliances, for performing a thorough investigation in accordance with an agreed timetable and for taking all the measures that are necessary to prevent recurrence of the non-compliances. 4.58. The regulatory body shall establish criteria for corrective actions, including enforcing the cessation of activities or the shutting down of a facility where necessary. On-site inspectors, if any, shall be authorized to take corrective action if there is an imminent likelihood of safety significant events. 4.59. In the event that unforeseen radiation risks are identified, whether or not they are due to non-compliances with regulatory requirements or authorization conditions, the regulatory body shall require the authorized party to take appropriate corrective actions to reduce the risks. 4.60. Finally, the regulatory body shall confirm that the authorized party has effectively implemented any necessary corrective actions.		

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
131	4	Requirement 32: Regulations and guides	The regulatory body shall establish or adopt regulations and guides to specify the principles, requirements and associated criteria for safety upon which its regulatory judgements, decisions and actions are based.			

138	5	Principle 3: Leadership and management for safety	Effective leadership and management for safety must be established and sustained in organizations concerned with, and facilities and activities that give rise to, radiation risks.	3.12. Leadership in safety matters has to be demonstrated at the highest levels in an organization. Safety has to be achieved and maintained by means of an effective management system. This system has to integrate all elements of management so that requirements for safety are established and applied coherently with other requirements, including those for human performance, quality and security, and so that safety is not compromised by other requirements or demands. The management system also has to ensure the promotion of a safety culture, the regular assessment of safety performance and the application of lessons learned from experience. 3.13. A safety culture that governs the attitudes and behaviour in relation to safety of all organizations and individuals concerned must be integrated in the management system. Safety culture includes: —Individual and collective commitment to safety on the part of the leadership, the management and personnel at all levels; —Accountability of organizations and of individuals at all levels for safety; —Measures to encourage a questioning and learning attitude and to discourage complacency with regard to safety. 3.14. An important factor in a management system is the recognition of the entire range of interactions of individuals at all levels with technology and with organizations. To prevent human and organizational failures, human factors have to be taken into account and good performance and good practices have to be supported. 3.15. Safety has to be assessed for all facilities and activities, consistent with a graded approach. Safety assessment involves the systematic analysis of normal operation and its effects, of the ways in which failures might occur and of the consequences of such failures. Safety assessments cover the safety measures necessary to control the hazard, and the design and engineered safety features are assessed to demonstrate that they fulfil the safety functions required of them. Where control measures or operator actions are called on to maintain safety, an initial safety assessment has to be carried out to demonstrate that the arrangements made are robust and that they can be relied on. A facility may only be constructed and commissioned or an activity may only be commenced once it has been demonstrated to the satisfaction of the regulatory body that the proposed safety measures are adequate. 3.16. The process of safety assessment for facilities and activities is repeated in whole or in part as necessary later in the conduct of operations in order to take into account changed circumstances (such as the application of new standards or scientific and technological developments), the feedback of operating experience, modifications and the effects of ageing. For operations that continue over long periods of time, assessments are reviewed and repeated as necessary. Continuation of such operations is subject to these reassessments demonstrating to the satisfaction of the regulatory body that the safety measures remain adequate. 3.17. Despite all measures taken, accidents may occur. The precursors to accidents have to be identified and analysed, and measures have to be taken to prevent the recurrence of accidents. The feedback of operating experience from facilities and activities — and, where relevant, from elsewhere — is a key means of enhancing safety. Processes must be put in place for the feedback and analysis of operating	Ineffective management system Lack of a safety culture Human factors not taken into account in decision making Lack of safety assessment of all facilities and activities consistent with a graded approach Lack of identification, analysis and actions based on precursors to accidents including relevant operating experience	Effective safety management system Robust safety culture Decision making taking human factors into account A graded approach to safety assessment that covers all facilities and activities Effective performance monitoring and continuous improvement that identifies, analyzes and takes actions on accident precursors

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				experience, including initiating events, accident precursors, near misses, accidents and unauthorized acts, so that lessons may be learned, shared and acted upon.		
139	5	Principle 4: Justification of facilities and activities	Facilities and activities that give rise to radiation risks must yield an overall benefit.	3.18. For facilities and activities to be considered justified, the benefits that they yield must outweigh the radiation risks to which they give rise. For the purposes of assessing benefit and risk, all significant consequences of the operation of facilities and the conduct of activities have to be taken into account. 3.19. In many cases, decisions relating to benefit and risk are taken at the highest levels of government, such as a decision by a State to embark on a nuclear power programme. In other cases, the regulatory body may determine whether proposed facilities and activities are justified. 3.20. Medical radiation exposure of patients — whether for diagnosis or treatment — is a special case, in that the benefit is primarily to the patient. The justification for such exposure is therefore considered first with regard to the specific procedure to be used and then on a patient by patient basis. The justification relies on clinical judgement as to whether a diagnostic or therapeutic procedure would be beneficial. Such clinical judgement is mainly a matter for medical practitioners. For this reason, medical practitioners must be properly trained in radiation protection.	Lack of taking all significant consequences into account when determining the tolerability of the risk from the dangerous technology.	Tolerability of risks from dangerous technologies takes into account all significant consequences

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
140	5	Principle 5: Optimization of protection	Protection must be optimized to provide the highest level of safety that can reasonably be achieved.	3.21. The safety measures that are applied to facilities and activities that give rise to radiation risks are considered optimized if they provide the highest level of safety that can reasonably be achieved throughout the lifetime of the facility or activity, without unduly limiting its utilization. 3.22. To determine whether radiation risks are as low as reasonably achievable, all such risks, whether arising from normal operations or from abnormal or accident conditions, must be assessed (using a graded approach) a priori and periodically reassessed throughout the lifetime of facilities and activities. Where there are interdependences between related actions or between their associated risks (e.g. for different stages of the lifetime of facilities and activities, for risks to different groups or for different steps in radioactive waste management), these must also be considered. Account also has to be taken of uncertainties in knowledge. 3.23. The optimization of protection requires judgements to be made about the relative significance of various factors, including: —The number of people (workers and the public) who may be exposed to radiation; —The likelihood of their incurring exposures; —The magnitude and distribution of radiation doses received; —Radiation risks arising from foreseeable events; —Economic, social and environmental factors. The optimization of protection also means using good practices and common sense to avoid radiation risks as far as is practical in day to day activities. 3.24. The resources devoted to safety by the licensee, and the scope and stringency of regulations and their application, have to be commensurate with the magnitude of the radiation risks and their amenability to control. Regulatory control may not be needed where this is not warranted by the magnitude of the radiation risks.	Risk is not kept at the lowest level that is reasonably achievable	All reasonable efforts are undertaken to reduce risk to the lowest level achievable
141	5	Principle 6: Limitation of risks to individuals	Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.	3.25. Justification and optimization of protection do not in themselves guarantee that no individual bears an unacceptable risk of harm. Consequently, doses and radiation risks must be controlled within specified limits. 3.26. Conversely, because dose limits and risk limits represent a legal upper bound of acceptability, they are insufficient in themselves to ensure the best achievable protection under the circumstances, and they therefore have to be supplemented by the optimization of protection. Thus both the optimization of protection and the limitation of doses and risks to individuals are necessary to achieve the desired level of safety.	Inadequate control of risks within specified limits	Control of risks to within specified limits

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
142	5	Principle 7: Protection of present and future generations	People and the environment, present and future, must be protected against radiation risks.	3.27. Radiation risks may transcend national borders and may persist for long periods of time. The possible consequences, now and in the future, of current actions have to be taken into account in judging the adequacy of measures to control radiation risks. In particular: —Safety standards apply not only to local populations but also to populations remote from facilities and activities. —Where effects could span generations, subsequent generations have to be adequately protected without any need for them to take significant protective actions. 3.28. Whereas the effects of radiation exposure on human health are relatively well understood, albeit with uncertainties, the effects of radiation on the environment have been less thoroughly investigated. The present system of radiation protection generally provides appropriate protection of ecosystems in the human environment against harmful effects of radiation exposure. The general intent of the measures taken for the purposes of environmental protection has been to protect ecosystems against radiation exposure that would have adverse consequences for populations of a species (as distinct from individual organisms). 3.29. Radioactive waste must be managed in such a way as to avoid imposing an undue burden on future generations; that is, the generations that produce the waste have to seek and apply safe, practicable and environmentally acceptable solutions for its long term management. The generation of radioactive waste must be kept to the minimum practicable level by means of appropriate design measures and procedures, such as the recycling and reuse of material.	Lack of taking into account the impact of risks across national borders and/or the long term impacts on future generations	Risk management practices take into account the consequence across national borders and take into account the long term impacts on future generations

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
143	5	Principle 8: Prevention of accidents	All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.	3.30. The most harmful consequences arising from facilities and activities have come from the loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or other source of radiation. Consequently, to ensure that the likelihood of an accident having harmful consequences is extremely low, measures have to be taken: —To prevent the occurrence of failures or abnormal conditions (including breaches of security) that could lead to such a loss of control; —To prevent the escalation of any such failures or abnormal conditions that do occur; —To prevent the loss of, or the loss of control over, a radioactive source or other source of radiation. 3.31. The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'. Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of defence in depth. 3.32. Defence in depth is provided by an appropriate combination of: —An effective management system with a strong management commitment to safety and a strong safety culture. —Adequate site selection and the incorporation of good design and engineering features providing safety margins, diversity and redundancy, mainly by the use of: • Design, technology and materials of high quality and reliability; • Control, limiting and protection systems and surveillance features; • An appropriate combination of inherent and engineered safety features. —Comprehensive operational procedures and practices as well as accident management procedures. 3.33. Accident management procedures must be developed in advance to provide the means for regaining control over a nuclear reactor core, nuclear chain reaction or other source of radiation in the event of a loss of control and for mitigating any harmful consequences.	Risk is not kept at the lowest level that is reasonably achievable	All reasonable efforts are undertaken to reduce risk to the lowest level achievable A defence-in-depth strategy is implemented to prevent and mitigate possible accidents

146	6	3.1.1. Safety culture	Principle: An established safety culture governs the actions and interactions of all individuals and organizations engaged in activities related to nuclear power.	31. The phrase ‘safety culture’ refers to a very general matter, the personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety of nuclear power plants. The starting point for the necessary full attention to safety matters is with the senior management of all organizations concerned. Policies are established and implemented which ensure correct practices, with the recognition that their importance lies not just in the practices themselves but also in the environment of safety consciousness which they create. Clear lines of responsibility, communication, and authority backed up with adequate resources are established; sound procedures are developed; strict adherence to these procedures is demanded; internal reviews are performed of safety related activities; above all, staff training and education emphasize the reasons behind the safety practices established, together with the consequences for safety of shortfalls in personal performance. The arrangements for the management of safety are documented as described in INSAG-13, ‘Management of Operational Safety in Nuclear Power Plants’. 32. These matters are especially important for operating organizations and the staff directly engaged in plant operation. For the latter, at all levels, training emphasizes the significance of their individual tasks from the standpoint of basic understanding and knowledge of the plant and the equipment at their command, with special emphasis on the reasons underlying safety limits and the safety consequences of violations. Open attitudes are required in such staff to ensure that information relevant to plant safety is freely communicated; when errors of practice are committed, their admission is particularly encouraged. By these means, an all pervading safety thinking is achieved, allowing an inherently questioning attitude, the learning from experience, the prevention of complacency, a commitment to excellence, and the fostering of both personal accountability and corporate self-regulation in safety matters. 34. A good nuclear safety culture has the following characteristics: —When any possible conflict in priority arises, safety and quality take precedence over schedule and cost. —Errors and near misses when committed are seen not only as a matter of concern but also as a source of experience from which benefit can be derived. Individuals are encouraged to identify, report and correct imperfections in their own work in order to help others as well as themselves to avert future problems. —Plant changes or activities are conducted in accordance with procedures. If any doubt arises about the procedures, the evolution is terminated by returning the plant to a safe and stable condition. The procedures are evaluated and changed if necessary before proceeding further. —When problems are identified, the emphasis is placed upon understanding the root cause of the problems and finding the best solutions without being diverted by who identified or contributed to the problem; the objective is to find ‘what is right’ and not ‘who is right’. —The goal of supervisory and management personnel is that every task be done right the first time. They are expected to accept and insist upon full accountability for the success of each work activity and to be involved in the work to the extent necessary to achieve success. —Practices and policies convey an attitude of trust and an approach that supports teamwork at all levels and reinforces positive attitudes towards safety.	Individuals engaged in safety related activities do not adequately take safety into account in their decision making	An established safety culture governs the actions and interactions of all individuals and organizations engaged in safety related activities

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				—Feedback is solicited from station personnel and contractors to help identify concerns, impediments and opportunities to improve. Management reinforces an attitude of individual behaviour that leads staff to identify problems promptly and fully. —The organization has a commitment to continuous safety improvement and to manage change effectively. —Senior managers prevent isolationism and encourage the establishment of a learning organization. —Every individual, every supervisor and every manager demonstrates personal integrity at every opportunity that arises during the lifetime of the nuclear power plant. —Every plant change, every meeting and every safety assessment is taken as an opportunity to teach, learn and reinforce the preceding characteristics and principles.		
148	6	3.1.3 Regulatory control and independent verification	Principle: The government establishes the legal framework for a nuclear industry and an independent regulatory organization which is responsible for licensing and regulatory control of nuclear power plants and for enforcing the relevant regulations. The separation between the responsibilities of the regulatory organization and those of other parties is clear, so that the regulators retain their independence as a safety authority and are protected from undue pressure.	40. A legally constituted regulatory organization provides governmental licensing, regulation and surveillance of the operation of nuclear power plants in respect of their safety. Activities of the regulatory organizations cover the following functional areas: —specification and development of standards and regulations for safety; —issue of licences to operating organizations, following appropriate assessments of nuclear safety, the financial viability of the applicant and its organizational and managerial capabilities; —inspection, monitoring and review of the safety performance of nuclear plants and operating organizations; —requiring corrective actions of an operating organization where necessary and taking any necessary enforcement actions, including withdrawal of licence, if acceptable safety levels are not achieved; —advocacy of safety research, as discussed in Section 3.3.8; and —dissemination of safety information (also discussed in Section 3.3.8). 41. The regulatory organization acts independently of designers, constructors and operators to the extent necessary to ensure that safety is the only mission of the regulatory personnel. The resources of the regulatory organization are sufficient for it to accomplish its functions without adversely affecting construction schedules or energy production, except where warranted for the assurance of safety. Expertise in a sufficiently wide range of nuclear technologies is available to the regulatory organization. 42. The regulatory organization does not attempt to take the primary responsibility for safe operation away from the operating organization, recognizing that such action has the potential to reduce safety levels. 43. To fulfil its functions effectively, the regulatory organization has the necessary legal authority, and it is provided with free access to facilities and to relevant information in the possession of the operating organization.		The government establishes the legal framework for a nuclear industry and an independent regulatory organization which is responsible for licensing and regulatory control

149	6	3.2.1. Defence in depth	Principle: To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.	47. The defence in depth concept provides an overall strategy for safety measures and features of nuclear power plants. When properly applied, it ensures that no single human or equipment failure would lead to harm to the public, and even combinations of failures that are only remotely possible would lead to little or no harm. Defence in depth helps to establish that the three basic safety functions (controlling the power, cooling the fuel and confining the radioactive material) are preserved, and that radioactive materials do not reach people or the environment. 48. The principle of defence in depth is implemented primarily by means of a series of barriers which would in principle never be jeopardized, and which must be violated in turn before harm can occur to people or the environment. These barriers are physical, providing for the confinement of radioactive material at successive locations. The barriers may serve operational and safety purposes, or may serve safety purposes only. Power operation is only allowed if this multibarrier system is not jeopardized and is capable of functioning as designed. 49. The strategy for defence in depth is twofold: first, to prevent accidents and second, if prevention fails, to limit the potential consequences of accidents and to prevent their evolution to more serious conditions. Defence in depth is generally structured in five levels. The objectives of each level of protection and the essential means of achieving them in existing plants are shown in Table I, which is reproduced from INSAG-10. If one level were to fail, the subsequent level comes into play, and so on. Special attention is paid to hazards that could potentially impair several levels of defence, such as fire, flooding or earthquakes. Precautions are taken to prevent such hazards wherever possible and the plant and its safety systems are designed to cope with them. 50. The reliability of the physical barriers is enhanced by applying the concept of defence in depth to them in turn, protecting each of them by a series of measures. Each physical barrier is designed conservatively, its quality is checked to ensure that the margins against failure are retained, its status is monitored, and all plant processes capable of affecting it are controlled and monitored in operation. Human aspects of defence in depth are brought into play to protect the integrity of the barriers, such as quality assurance, administrative controls, safety reviews, independent regulation, operating limits, personnel qualification and training, and safety culture. Design provisions including both those for normal plant systems and those for engineered safety systems help to prevent undue challenges to the integrity of the physical barriers, to prevent the failure of a barrier if it is jeopardized, and to prevent consequential damage of multiple barriers in series. Safety system designers ensure to the extent practicable that the different safety systems protecting the physical barriers are functionally independent under accident conditions. 51. All the levels of defence are available at all times that a plant is at normal power. Appropriate levels are available at other times. The existence of several levels of defence in depth is never justification for continued operation in the absence of one level. Severe accidents in the past have been the result of multiple failures, both human and equipment failures, due to deficiencies in several components of defence in depth that should not have been permitted. 52. System design according to defence in depth includes process controls that use feedback to provide a tolerance of any failures which might otherwise allow faults or abnormal conditions to develop into accidents. These controls protect the	The implementation of a defence in depth strategy is not adequate to prevent the release of radioactive material to the environment.	To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				physical barriers by keeping the plant in a well defined region of operating parameters where barriers will not be jeopardized. Care in system design prevents cliff edge effects which might permit small deviations to precipitate grossly abnormal plant behaviour and cause damage. 53. Competent engineering of the barriers and the measures for their protection coupled with feedback to maintain operation in optimal ranges leads to a record of smooth, steady performance in producing electricity on demand. This indicates the proper implementation of the most important indicator of the success of defence in depth, which is operation with little or no need to call on safety systems. 54. The multibarrier system protects humans and the environment in a wide range of abnormal conditions. Preplanned countermeasures are provided, as a further component of defence in depth, against the possibility that radioactive material might still be released from the plant. 55. The Appendix presents a discussion of the means by which the separate components of defence in depth protect and complement each other. The importance of prevention and mitigation of accidents in defence in depth is treated in the following two corollaries.		

150	6	3.2.2. Accident prevention	Principle: Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents, particularly any which could cause severe core damage.	57. The design, construction, operation and maintenance of nuclear power plants has as its primary objective the generation of electricity reliably and economically. In accordance with the general safety management principle on safety culture, the safety implications of decisions in all these areas must be borne in mind. The following is concentrated on these safety aspects. 58. The first means of preventing accidents is to strive for such high quality in design, construction and operation of the plant that deviations from normal operational states are infrequent. Safety systems are used as a backup to feedback in process control to prevent such deviations from developing into accidents. Safety systems make use of redundancy and diversity of design and the physical separation of parallel components, where appropriate, to reduce the likelihood of the loss of a vital safety function. Systems and components are inspected and tested regularly to reveal any degradation which might lead to abnormal operating conditions or inadequate safety system performance. Abnormal conditions possibly affecting nuclear safety are promptly detected by monitoring systems that give alarms and in many cases initiate corrective actions automatically. The second means of preventing accidents is to foster a questioning attitude from the staff and to promote discussion of what could go wrong prior to initiating activities. The operators are trained to recognize readily the onset of an accident and to respond properly and in a timely manner to such abnormal conditions. They have also been well trained in appropriate operating procedures, with which they have become familiarized. 59. Thus the prevention of accidents depends on conservatively designed equipment and good operational practices to prevent failure, quality assurance to verify the achievement of the design intent, surveillance to detect degradation or incipient failure during operation, and steps to ensure that a small perturbation or incipient failure would not develop into a more serious situation. 60. A number of PSAs have been made for a range of nuclear power plant designs in different countries. They show that sufficiently low probabilities of severe core damage are attainable in some designs. When effective preparation for accident management and for mitigation of the effects of severe accidents is taken into account, the results of these PSAs are consistent with the general nuclear safety objective stated in Section 2.1. 61. PSA also guides design and operation by identifying potential accident sequences that contribute to risk. Measures can then be taken to reduce this contribution. 62. The scope of PSA has been expanded into several new areas to prevent and reduce the occurrence of accidents: —As a number of significant events occurred at shutdown or at low power, they were analysed by PSA which showed, as reported in INSAG-10, that in some cases the associated risk (contribution to frequency of core damage) is comparable with that associated with full power operation. PSA is now increasingly used to minimize risks associated with shutdown and low power by maintaining adequate defence in depth and the proper system availability to support the key safety functions of control of reactivity, shutdown cooling, maintenance of coolant inventory, maintenance of electrical power, spent fuel cooling, containment and maintenance of critical support systems. —PSA is being employed to analyse the various plant systems, structures and	The plant design does not adequately eliminate hazards or prevent accidents from occurring.	Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents Hazards shall be eliminated if possible Remaining hazards shall be controlled to make their probability of occurrence as low as reasonably achievable

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				components that are important for safety and to assess remedial actions when their performance is not satisfactory. PSA is used to evaluate diversity in systems and to prioritize resources to ensure that the most important components receive their proportionate share of available resources. —PSA is beginning to be employed to develop risk informed safety programme strategies (e.g. in-service inspection). In all such novel applications, PSA is used as another important technique to complement engineering judgement, experience, defence in depth concepts and design basis considerations. Also, as the uses of PSA increase, it is important that the models, the database and the calculations of PSA be kept accurate over the lifetime of the plants.		
151	6	3.2.3. Accident mitigation	Principle: In-plant and off-site mitigation measures are available and are prepared for that would substantially reduce the effects of an accidental release of radioactive material.	64. Provisions for accident mitigation extend the defence in depth concept beyond accident prevention. The accident mitigation provisions are of three kinds, namely, accident management, engineered safety features and off-site countermeasures. 65. Accident management includes preplanned and ad hoc operational practices which, in circumstances in which the design specifications of the plant are exceeded, would make optimum use of existing plant equipment in normal and unusual ways to restore control. This phase of accident management would have the objective of restoring the plant to a safe state with the reactor shut down, continued fuel cooling ensured, radioactive material confined and the confinement function protected. In such circumstances, engineered safety features would act to confine any radioactive material released from the core so that discharges to the environment would be minimal. These engineered safety features include physical barriers, some of which have the single purpose of confining radioactive material. Off-site countermeasures are available, going beyond the level of protection provided in most human endeavours, to compensate for the remote possibility that safety measures at the plant might fail. In such a case, the effects on the surrounding population or the environment would be mitigated by protective actions, such as sheltering or evacuation of the population, and by prevention of the transfer of radioactive material to humans by food-chains and other pathways. 66. Accident management in operating plants is being extended into the realm of increasingly severe accidents. This requires additional guidelines or procedures, further understanding of the prevailing phenomena, appropriate assignment of responsibilities, and training for managing accidents of increased severity. Designers and owners of future plants are seeking even more improvements in reducing off-site radiological releases, as discussed in paras 25 and 27.	In-plant and off-site mitigation measures are inadequate to substantially reduce the effects of an accident.	In-plant and off-site mitigation measures are available and are prepared for that would substantially reduce the effects of an accident.

160	6	3.3.9. Operational excellence	Principle: Operational excellence is achieved in present and future nuclear power plant operations by: augmenting safety culture and defence in depth; improving human performance; maintaining excellent material condition and equipment performance; using self-assessments and peer reviews; exchanging operating experience and other information around the world; increasing application of PSAs; and extending the implementation of severe accident management.	117. Several of the proposed improvements in the operational excellence principle have been covered elsewhere: safety culture (paras 33 and 34); defence in depth (para. 49); self-assessment (paras 83–85); peer reviews (paras 86–88); human performance (para 93); PSA (paras 62 and 102); operating experience (para. 112); research (para. 114); severe accident mitigation (paras 66 and 102). These improvements are applicable to existing as well as future nuclear power plants. 118. Most of the preceding enhancements are aimed at improving human performance since a large fraction of plant events are caused by human error. Errors may be the result of the behaviour of a single individual, the collective behaviour of individuals, or the influences of the work environment, the organization or the management. Excellence in human performance is attained when all the individuals involved exhibit desirable behaviour and when the emphasis is put upon fostering or displaying a questioning attitude; reinforcing such desirable behaviour; encouraging leadership and promoting teamwork. 119. Several lessons have been learned from power plants striving for operational excellence. For instance, in seeking to obtain safety improvements to existing installations, account is taken of the balance between benefits and drawbacks (including costs). When the drawbacks of modifications far outweigh the likely gain in safety, generally they would not be undertaken. Also, account needs to be taken of the implications of changes for the usefulness of the experience gained and training developed in operating the plant in its existing configuration. Another example is that of organizational changes which can have the potential either to improve or to impair safety performance. It is important to ensure, prior to implementation, that the effect of the proposed changes will not reduce safety, either when the change has been completed or during the transitional period while it is being implemented. Under all such circumstances, leadership and quality of management are essential as well as the ability to involve staff throughout the entire organization. 120. Another important characteristic of operational excellence is the adoption of a strong preventive and predictive maintenance strategy which, for example, detects ageing and performance related problems in their early stages and corrects them before they have a significant impact on safety. It is important to show that the lifetime of the nuclear power plant is being managed to maintain safety so that the plant operating organization can make a valid up to date safety case. This process identifies systems, structures and components important to safety as well as non-safety-related systems, structures and components that directly support the safety related functions or are important to the performance of the balance of plant. The programme will show whether the measured or analysed degradation due to prevailing ageing mechanisms is acceptable in terms of safety. Furthermore, it would include an evaluation of time limited ageing analyses (e.g. allowable thermal cycles) and a demonstration that they are still applicable. Many of the considerations relating to ageing can be dealt with by non-destructive and other testing and examinations of nuclear power plants that are currently required. A proactive attitude, however, ensures that there is an all inclusive ageing programme which focuses upon operating experience problems associated with ageing and all the detectable and potentially significant adverse effects of ageing upon safety.	The performance of the operating organization is not consistent with best practice in the nuclear industry.	Operational excellence is achieved by: augmenting safety culture and defence in depth; improving human performance; maintaining excellent material condition and equipment performance; using self-assessments and peer reviews; exchanging operating experience and other information around the world; increasing application of PSAs; and extending the implementation of severe accident management.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
				121. Another consideration is the reduced demand for power and the development of alternative means of generation in some countries. This means that there is a decrease in the demand for engineering skills required to design, construct, commission and operate nuclear power plants. This can lead to a loss of expertise and particularly a loss of corporate memory. Operational excellence recognizes the need for processes to manage the changes arising from such loss of expertise. They include the identification of core skills to ensure safety and arrangements to preserve those core skills by training of less experienced engineers, by the use of mentors and by exchanging resources with other organizations. 122. Measurable indicators of safety performance are used in attaining operational excellence. The indicators are employed by management to trend plant safety and performance and to compare them with other plants performing at a very high level. 123. To be effective and permanent, the drive to operational excellence must come from within the operating organization, the management and its staff. The attainment of operational excellence has often been associated with increasing plant availability and reducing operating costs by streamlining and simplifying processes. However, it is essential that such gains be achieved with no reduction in overall plant safety.		
168	6	4.2.2.1. Plant process control systems	Principle: Normal operation and anticipated operational occurrences are controlled so that plant and system variables remain within their operating ranges. This reduces the frequency of demands on the safety systems.	165. Important plant neutronic and thermal–hydraulic variables have assigned operating ranges, trip set points and safety limits. The safety limits are extreme values of the variables at which conservative analysis indicates that undesirable or unacceptable damage to the plant may be initiated. The trip set points are at less extreme values of the variables which, if attained as a result of an anticipated operational occurrence or an equipment malfunction or failure, would actuate an automatic plant protective action such as a programmed power reduction, plant shutdown or an even more marked response (see the principle in Section 4.2.2.2 on automatic safety systems). Trip set points are chosen such that plant variables would not reach safety limits. The operating range, which is the domain of normal operation, is bounded by values of the variables less extreme than the trip set points. Automatic controls are kept operational to keep parameters within prescribed ranges. Deficiencies that affect automatic controls are resolved expeditiously. 166. It is important that trip actions are not induced too frequently, especially when they are not required for protection of the plant or the public. Not only would this interfere with the normal, productive use of the plant, but it could also compromise safety by the effects of sudden and precipitous changes, and it could induce excessive wear which might impair the reliability of safety systems. 167. Therefore, the more important neutronic and thermal–hydraulic variables are automatically maintained in the operating range. This is done by feedback systems acting on electrical and mechanical controls when variables begin to depart from the operating range. The normal operating state is then restored. The limits to the normal operating range are chosen so that the feedback action prevents variables from reaching trip set points in normal operation.	Lack of Adequately Defined and Executed Safety Management Plan Plant design and implementation is inadequate to control abnormal operations or to detect equipment failures.	Normal operation and anticipated operational occurrences are controlled so that plant and system variables remain within their operating ranges.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
200	6	4.5.5. Operational limits and conditions	Principle: A set of operational limits and conditions is defined to identify safe boundaries for plant operation. Minimum requirements are also set for the availability of staff and equipment.	285. As discussed in Section 4.2.2.1, a set of inviolable safety limits defines the extremes of the region of operating variables and conditions within which conservative analysis shows that the plant will not suffer undesirable effects or unacceptable damage. Operational limits for normal operation and trip points as necessary are set on key plant variables which are controlled by automatic systems. To ensure that anticipated transients do not lead to infringement of the safety limits, the operational limits and trip points are set conservatively on the basis of reliable analysis. Operational limits and conditions are defined for all the stages of commissioning, power operation, shutdown, shutting down, starting up, maintenance, testing and refuelling. Scheduled tests and inspections are performed to recalibrate instruments measuring and displaying the values of variables which have safety limits, and to check the correctness of trip points. 286. Additional conditions ensure that safety systems are either in operation or ready for use. These conditions are defined according to the reliability and the response expected of the systems. Minimum staffing requirements are also laid down, including, importantly, staffing requirements for the control room. These conditions may be temporarily suspended only for well justified testing or other special purposes, with compensating provisions and with prior safety analysis and approval at a level appropriate to he safety significance of the issue. 287. The original set of operational limits or conditions as well as any subsequent changes are subject to safety review and approval by the operating organization and the regulatory organization according to their safety significance. As a vital part of safety culture, it is essential that plant personnel understand the reasons for the safe limits of operation and the consequences of violation. Operational limits may not be infringed deliberately except in accordance with formal procedures that ensure both full recognition of the safety implications and provision of any necessary compensating factors.	Operating limits and conditions are not well documented, and/or do not cover all necessary limits and conditions Operating limits and conditions are not consistent with design assumptions and intent Operating limits and conditions were not revised to take into account operating experience Personnel responsible for conduct of safety related activities did not have a complete understanding of the operating limits and conditions Deviations from operating limits and conditions were not detected and/or appropriate remedial actions were not taken	A set of operational limits and conditions is defined to identify safe boundaries for plant operation.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
205	6	4.5.10. Feedback of operating experience	Principle: Plant management institutes measures to ensure that events significant for safety are detected and evaluated in depth, and that any necessary corrective measures are taken promptly and information on them is disseminated. The plant management has access to operational experience relevant to plant safety from other nuclear power plants around the world.	300. The importance for safety of an effective programme for the feedback of operational experience has been stressed in the fundamental principle in Section 3.3.8 related to operating experience and safety research. The plant manager reports promptly to the top management of the operating organization and to the regulatory organization any abnormal occurrence of significance for safety so that its implications can be properly analysed, the root cause identified and the information communicated to other nuclear power plants. Good operating practices, when judged to have potentially significant benefits for safety, are also reported in an appropriate way. 301. Independently of the generic analyses which may follow an abnormal and potentially damaging occurrence, the plant manager takes the necessary measures to prevent the recurrence of similar events at the plant, or at least takes measures to ensure that its repetition would not lead to an accident. Any corresponding modification, of either hardware or procedures, is made only after a safety assessment shows that the change will not jeopardize plant safety and after measures are taken to ensure quality appropriate to the safety significance. 302. Plant management personnel use the safety information gained from the operating experience of other nuclear power plants as a source of lessons applicable at their own plants to improve plant safety. 303. Regular maintenance and surveillance by the plant staff or by personnel at other similar plants is a source of information on safety related systems and components. Pooling of information through owners' groups is helpful in this way. The information is compiled and processed, and submitted to trend analysis either at the plant or in co-operation with other similar plants to identify incipient faults or degradation, such as those due to ageing. Measures are taken to prevent failures or to reverse adverse trends revealed by the processing of such information. 304. Plant management is aware of the safety significance of risk assessment for the plant, and co-operates in the performance of risk assessments by contributing the data needed.	The performance of the operating organization is not consistent with best practice in the nuclear industry.	Plant management institutes measures to ensure that events significant for safety are detected and evaluated in depth, and that any necessary corrective measures are taken promptly and information on them is disseminated. The plant management has access to operational experience relevant to plant safety from other nuclear power plants around the world.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
208	6	4.6.1. Strategy for accident management	Principle: The results of an analysis of the response of the plant to potential accidents beyond the design basis are used in preparing guidance on an accident management strategy.	319. Analysis is made of accidents beyond the design basis that have potential for severe core degradation and failure of barriers preventing the release of radioactive material. The symptoms of specific accidents are identified for use in diagnosis. Measures to be taken to reduce significantly the extent of plant damage or the effects of radiation are also identified. These might use normal plant systems in normal or unusual ways or special plant features provided especially for accident management. 320. Continued analysis of severe accidents and additional research and development tests to simulate them are increasing the available knowledge of severe accident behaviour. A typical example is the large international effort to carry out experimental and analytical studies of the presence of water on the outside surface of the pressure vessel (of a pressurized water reactor), in order to establish the cooling effectiveness as a function of vessel size. Such activities lead to new physical measures and/or extend the guidance provided for severe accident management. 321. As the severity of an accident increases and its likelihood of occurrence decreases, the measures to be taken become less certain and more difficult to specify because they depend upon plant specific characteristics. Plant design layout, capability, location and redundancy of plant emergency systems, availability of auxiliary heat sinks and other features of the balance of plant determine the success or failure of a prescribed strategy for severe accident management. Similarly, the ability of the containment to withstand a potential overpressure, the elevation of the reactor pressure vessel, the geometry and size of the reactor cavity, and the geometry of sumps have a role in strategic decisions to preserve containment integrity. These factors are taken into account in extending the guidance for severe accident management. 322. In future plants, the objectives of paras 25 and 27 will be applied to the prevention and mitigation of severe accidents and they will influence the degree and scope of accident management for such plants.	The analysis of the response of the plant to potential accidents beyond the design basis are inadequate to prepare guidance on an accident management strategy.	The results of an analysis of the response of the plant to potential accidents beyond the design basis are used in preparing guidance on an accident management strategy.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
210	6	4.6.3. Engineered features for accident management	Principle: Equipment, instrumentation and diagnostic aids are available to operators, who may at some time be faced with the need to control the course and consequences of an accident beyond the design basis.	327. The development of abnormal plant behaviour following equipment malfunction or operator error could be rapid in some circumstances. The operating staff would then have to diagnose the cause quickly and plan appropriate corrective action. Equipment is provided especially to assist in this. It comprises instrumentation reading out in the control room, environmentally qualified and capable of providing the information needed to recognize abnormal conditions, to correct faults and to determine the effects of corrective action. Examples of instrumentation provided specifically for accident management are coolant inventory trending systems for pressurized water reactors, monitors for very high containment pressure, hydrogen monitors and monitors of activity in primary coolant. 328. The capability for accident mitigation has always been important in nuclear plant design. The use of confinement structures and containment systems is evidence of this objective. Some of this equipment is useful in more extreme circumstances than envisaged in the original specifications because of the safety margin provided in design. Certain design changes to mitigate the effects of severe accidents have been made in recent years, concentrated on restoring and maintaining the core cooling and the confinement functions. These changes include the installation of filtered vents, hydrogen igniters and passive autocatalytic recombiners in some cases (see Table II).	The design of the information systems does not provide plant staff with adequate information for following and intervening in the course of an accident.	Equipment, instrumentation and diagnostic aids are available to operators, who may at some time be faced with the need to control the course and consequences of an accident beyond the design basis.
211	6	4.7. DECOMMISSIONING	Principle: Consideration is given in design and plant operations to facilitating eventual decommissioning and waste management. After the end of operations and the removal of spent fuel from the plant, radiation hazards are managed so as to protect the health of workers and the public during plant decommissioning.	330. A plant that is shut down remains an operating plant until its decommissioning and is subject to the normal control processes and procedures to ensure safety. In particular, the principles that govern a plant in a shutdown state apply (see Section 4.2.3.14). After the end of operations and the removal of spent fuel from the plant, a significant radiation hazard remains which must be managed to protect the health of workers and the public. The removal of plant equipment and its decontamination can be facilitated if appropriate consideration is given at the design stage to decommissioning and disposal of the wastes arising from decommissioning. Examples include using materials to minimize residual activity (on time-scales relevant for decommissioning) and to minimize the transport of radioactive material, thus minimizing the activation of long lived radionuclides, particularly those that are easily mobilized such as 36Cl and 14C, and designing for ease of removal. Such factors are now being taken into account during design for other reasons, such as ease of maintenance, replacement of components and minimization of worker doses. However, the implications of design choices and design changes for eventual decommissioning and waste disposal will also be considered in design audits during the design process. Similarly, during operations and maintenance, due attention is paid to the fact that the plant will ultimately be decommissioned. Thus, for example, good records are kept of contamination control and contamination incidents. Such records will facilitate the characterization and segregation of waste streams arising from decommissioning for disposal and facilitate planning for radiation protection during decommissioning. Finally, minimizing waste production as far as is reasonably practical during decommissioning is another means of limiting the volume of waste for disposal.	Inadequate consideration is given in design and plant operations to facilitating eventual decommissioning and waste management.	Consideration is given in design and plant operations to facilitating eventual decommissioning and waste management.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
212	6	4.8.1. Emergency plans	Principle: Emergency plans are prepared before the startup of the plant, and are exercised periodically to ensure that protection measures can be implemented in the event of an accident which results in, or has the potential for, significant releases of radioactive materials within and beyond the site boundary. Emergency planning zones defined around the plant allow for the use of a graded response.	334. Emergency plans are prepared for measures to be taken on and off the site to protect the public from any serious releases of radioactive materials from the plant. The plans are tested appropriately by exercising their communications and logistics and they are updated based upon experience. The tests are reviewed and witnessed, as appropriate by the regulator. The emergency plans define organizational arrangements and the division of responsibilities for emergency action, and they are flexible enough to be adapted to particular circumstances as they arise. 335. The emergency plans define the actions that would be taken in the event of a severe accident to re-establish control of the plant, to protect staff and the public, and to provide the necessary information speedily to the regulatory organization and other authorities. Emergency planning zones defined around the plant provide a basic geographical framework for decision making on implementing protective measures as part of a graded response. These measures include as required early notification, sheltering and evacuation, radioprotective prophylaxis and supply of protective equipment, radiation monitoring, control of ingress and egress, decontamination, medical care, provision of food and water, control of agricultural products, and dissemination of information.	Emergency plans for measures to be taken in the case of serious release of radioactive materials are not adequate.	Emergency plans are prepared before the startup of the plant, and are exercised periodically to ensure that protection measures can be implemented in the event of an accident
213	6	4.8.2. Emergency response facilities	Principle: A permanently equipped emergency centre is available off the site for emergency response. On the site, a similar centre is provided for directing emergency activities within the plant and communicating with the off-site emergency organization.	337. The off-site emergency centre is where all emergency action is determined and initiated, apart from on-site measures to bring the plant under control and protect staff. It has a reliable capability to communicate with the similar centre at the plant, with all important units of the emergency response organization, such as police and fire services, and governmental and public information sources. Since commercial telephone services may not be reliable in an emergency, other modes of communication are also available, such as dedicated telephone lines and radio transmission. Information on meteorology at the site and on radiation levels, if any, is provided to the emergency centres. Maps of the local area are available indicating the emergency planning zones and their characteristics. A means is available of permanently recording important information received and sent. 338. The on-site emergency centre is a location at which all on-site measures can be determined and initiated, apart from detailed control of the plant. It is equipped with instrumentation relaying important plant conditions. The centre is the location where data on plant conditions would be compiled for transmission to the off-site emergency centre. Protective equipment is provided for emergency personnel.	A adequate, permanently equipped emergency centre is not available off the site for emergency response. On the site, a similar centre is provided for directing emergency activities within the plant and communicating with the off-site emergency organization.	A permanently equipped emergency centre is available off the site for emergency response. On the site, a similar centre is provided for directing emergency activities within the plant and communicating with the off-site emergency organization.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
214	6	4.8.3. Assessment of accident consequences and radiological monitoring	Principle: Means are available to the responsible site staff to be used in early prediction of the extent and significance of any release of radioactive materials if an accident were to occur, for rapid and continuous assessment of the radiological situation, and for determining the need for protective measures.	340. Assessment methods are available to plant management that allow the prediction of the doses or potential doses that could result from an actual or a possible release of radioactive materials. On-site monitoring is used to characterize the source term and release rates. For off-site data, facilities are provided in the form of mobile radiological monitoring teams and in many cases a network of fixed monitoring stations. Facilities are also available for rapid analysis and interpretation of the levels and nature of activity in large numbers of samples. 341. Decisions on the need for protective measures are made on the basis of recommendations from the operating organization and intervention levels or guidelines set by competent national and international bodies. These authorities must receive relevant information speedily and be competent to make the judgements that may be necessary.	Means are not adequately available to the responsible site staff to be used in early prediction of the extent and significance of any release of radioactive materials if an accident were to occur, for rapid and continuous assessment of the radiological situation, and for determining the need for protective measures.	Means are available to the responsible site staff to be used in early prediction of the extent and significance of any release of radioactive materials if an accident were to occur, for rapid and continuous assessment of the radiological situation, and for determining the need for protective measures.
219	7	Level 5	5) Mitigation of radiological consequences of significant releases of radioactive materials	- Off-site emergency procedures are prepared in consultation with the operating organization and the authorities in charge and must comply with international agreements. - Both on-site and off-site emergency plans are exercised periodically to the extent necessary to ensure the readiness of the organizations involved.	- inadequate emergency procedures - inadequate emergency plans - inadequate training in emergency procedures	- emergency plans and procedures in compliance with international agreements - periodic exercising of emergency plans and procedures

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
220	7	Common	Common Prerequisites	- Conservatism - Conservatism is broadly applied at the first three levels of defence. Conservative assumptions are made for site selection, design and construction, commissioning and operation. Appropriate conservative assumptions and safety margins are also considered in the review of modifications, the assessment of ageing effects, periodic safety reassessment, and the development of emergency plans, as well as in regulatory review and subsequent licensing decisions. At Levels 4 and 5, best estimate considerations are increasingly important. - Quality Assurance - Each level of defence can be effective only if the quality of design, materials, structures, components and systems, operation and maintenance can be relied upon. Quality assurance programmes can ensure the development of a safe design (including site evaluation, design of process and safety systems, design of barriers, design of modifications and safety analysis). They can also ensure that the intent of the design is achieved in the plant as built and that the plant is being operated as intended and maintained as designed. - Safety Culture - Organizations and individuals involved in activities that may have an impact at each level of defence need to be committed to a strong safety culture (see Safety Culture, INSAG-4 [3]). The operating organization and the governmental organization, as well as organizations involved in design, manufacturing, construction, maintenance, testing and in-service inspection and emergency interventions, must ensure that appropriate prerequisites are met and that appropriate methods are used.	- lack of conservatism - lack of adequate quality assurance - poor safety culture	- Conservative assumptions are made for site selection, design and construction, commissioning and operation. - Appropriate conservative assumptions and safety margins are also considered in the review of modifications, the assessment of ageing effects, periodic safety reassessment, and the development of emergency plans, as well as in regulatory review and subsequent licensing decisions. - At Levels 4 and 5, best estimate considerations are increasingly important. - Quality assurance programmes ensure the development of a safe design (including site evaluation, design of process and safety systems, design of barriers, design of modifications and safety analysis). - They also ensure that the intent of the design is achieved in the plant as built and that the plant is being operated as intended and maintained as designed. - Organizations and individuals involved in activities that may have an impact at each level of defence need to be committed to a strong safety culture (see Safety Culture, INSAG-4 [3]). - The operating organization and the governmental organization, as well as organizations involved in design, manufacturing, construction, maintenance, testing and in-service inspection and emergency interventions, must ensure that appropriate prerequisites are met and that appropriate methods are used.

PERFORMANCE MONITORING & CONTINUOUS IMPROVEMENT

Business Process

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
81	1	Requirement 3: Safety of the plant design throughout the lifetime of the plant	The operating organization shall establish a formal system for ensuring the continuing safety of the plant design throughout the lifetime of the nuclear power plant.	3.5. The formal system for ensuring the continuing safety of the plant design shall include a formally designated entity responsible for the safety of the plant design within the operating organization's management system. Tasks that are assigned to external organizations (referred to as responsible designers) for the design of specific parts of the plant shall be taken into account in the arrangements. 3.6. The formally designated entity shall ensure that the plant design meets the acceptance criteria for safety, reliability and quality in accordance with relevant national and international codes and standards, laws and regulations. A series of tasks and functions shall be established and implemented to ensure the following: (a) That the plant design is fit for purpose and meets the requirement for the optimization of protection and safety by keeping radiation risks as low as reasonably achievable; (b) That the design verification, definition of engineering codes and standards and requirements, use of proven engineering practices, provision for feedback of information on construction and experience, approval of key engineering documents, conduct of safety assessments and maintaining a safety culture are included in the formal system for ensuring the continuing safety of the plant design; (c) That the knowledge of the design that is needed for safe operation, maintenance (including adequate intervals for testing) and modification of the plant is available, that this knowledge is maintained up to date by the operating organization, and that due account is taken of past operating experience and validated research findings; (d) That management of design requirements and configuration control are maintained; (e) That the necessary interfaces with responsible designers and suppliers engaged in design work are established and controlled; (f) That the necessary engineering expertise and scientific and technical knowledge are maintained within the operating organization; (g) That all design changes to the plant are reviewed, verified, documented and approved; (h) That adequate documentation is maintained to facilitate future decommissioning of the plant.	Design changes are made to the plant that do not satisfy safety requirements, or introduce new hazards that are not addressed adequately by the current design New technologies become available that enable reduction of radiation risk with a reasonable cost of implementation	Establish a safety management system that ensuring the continuing safety of the plant design. Designate an individual to be responsible for the safety of the plant design

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
82	2	Requirement 12: Periodic safety review	Systematic safety assessments of the plant, in accordance with the regulatory requirements, shall be performed by the operating organization throughout the plant's operating lifetime, with due account taken of operating experience and significant new safety related information from all relevant sources.	4.44. Safety reviews such as periodic safety reviews or safety assessments under alternative arrangements shall be carried out throughout the lifetime of the plant, at regular intervals and as frequently as necessary (typically no less frequently than once in ten years). Safety reviews shall address, in an appropriate manner: the consequences of the cumulative effects of plant ageing and plant modification; equipment requalification; operating experience, including national and international operating experience; current national and international standards; technical developments; organizational and management issues; and site related aspects. Safety reviews shall be aimed at ensuring a high level of safety throughout the operating lifetime of the plant. 4.45. The operating organization shall report to the regulatory body as required, in a timely manner, the confirmed findings of the safety review that have implications for safety. 4.46. The scope of the safety review shall include all safety related aspects of an operating plant. To complement deterministic safety assessment, probabilistic safety assessment (PSA) can be used for input to the safety review to provide insight into the contributions to safety of different safety related aspects of the plant. 4.47. On the basis of the results of the systematic safety assessment, the operating organization shall implement any necessary corrective actions and reasonably practicable modifications for compliance with applicable standards with the aim of enhancing the safety of the plant by further reducing the likelihood and the potential consequences of accidents.	Cumulative effect of plant ageing and plant modification result in non-compliance with safety requirements Operating experience in the plant and at other plants that identified non-compliances with safety requirements has not been taken into account Cumulative effect of changes to processes, organizations and governance result in non-compliance with safety requirements	Establish periodic safety reviews of the plant, processes, organizations and governance Establish continuous improvement process taking input from periodic safety review and operational experience both internal and external to the organization
83	2	Requirement 13: Equipment qualification	The operating organization shall ensure that a systematic assessment is carried out to provide reliable confirmation that safety related items are capable of the required performance for all operational states and for accident conditions.	4.48. Appropriate concepts and the scope and process of equipment qualification shall be established, and effective and practicable methods shall be used to upgrade and preserve equipment qualification. A programme to establish, to confirm and to maintain required equipment qualification shall be launched from the initial phases of design, supply and installation of the equipment. The effectiveness of equipment qualification programmes shall be periodically reviewed. 4.49. The scope and details of the equipment qualification process, in terms of the required inspection area(s), method(s) of non-destructive testing, possible defects inspected for and required effectiveness of inspection, shall be documented and submitted to the regulatory body for review and approval. Relevant national and international experience shall be taken into account in accordance with national regulations.	Non-compliance of equipment with safety requirements	Effective equipment qualification programs to provide confidence that equipment will satisfy its safety requirements

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
84	2	Requirement 24: Feedback of operating experience	The operating organization shall establish an operating experience programme to learn from events at the plant and events in the nuclear industry and other industries worldwide.	5.27. The operating organization shall establish and implement a programme to report, collect, screen, analyse, trend, document and communicate operating experience at the plant in a systematic way. It shall obtain and evaluate available information on relevant operating experience at other nuclear installations to draw and incorporate lessons for its own operations, including its emergency arrangements. It shall also encourage the exchange of experience within national and international systems for the feedback of operating experience. Relevant lessons from other industries shall also be taken into consideration, as necessary. 5.28. Events with safety implications shall be investigated in accordance with their actual or potential significance. Events with significant implications for safety shall be investigated to identify their direct and root causes, including causes relating to equipment design, operation and maintenance, or to human and organizational factors. The results of such analyses shall be included, as appropriate, in relevant training programmes and shall be used in reviewing procedures and instructions. Plant event reports and non-radiation-related accident reports shall identify tasks for which inadequate training may be contributing to equipment damage, excessive unavailability of equipment, the need for unscheduled maintenance work, the need for repetition of work, unsafe practices or lack of adherence to approved procedures. 5.29. Information on operating experience shall be examined by competent persons for any precursors to, or trends in, adverse conditions for safety, so that any necessary corrective actions can be taken before serious conditions arise. 5.30. As a result of the investigation of events, clear recommendations shall be developed for the responsible managers, who shall take appropriate corrective actions in due time to avoid any recurrence of the events. Corrective actions shall be prioritized, scheduled and effectively implemented and shall be reviewed for their effectiveness. Operating personnel shall be briefed on events of relevance and shall take the necessary corrective actions to make their recurrence less likely. 5.31. The operating organization shall be responsible for instilling an attitude among plant personnel that encourages the reporting of all events, including low level events and near misses, potential problems relating to equipment failures, shortcomings in human performance, procedural deficiencies or inconsistencies in documentation that are relevant to safety. 5.32. The operating organization shall maintain liaison, as appropriate, with support organizations (e.g. manufacturers, research organizations and designers) involved in the design, construction, commissioning and operation of the plant in order to feed back information on operating experience and to obtain advice, if necessary, in the event of equipment failure or in other events. 5.33. The operating experience programme shall be periodically evaluated to determine its effectiveness and to identify any necessary improvements.	Operating experience in the plant and at other plants that identified non-compliances with safety requirements has not been taken into account	Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner. Establish a program to investigate events with significant implications for safety and take effective actions to avoid reoccurrence of the events.

85	2	Requirement 8: Performance of safety related activities	The operating organization shall ensure that safety related activities are adequately analysed and controlled to ensure that the risks associated with harmful effects of ionizing radiation are kept as low as reasonably achievable.	4.25. All routine and non-routine operational activities shall be assessed for potential risks associated with harmful effects of ionizing radiation. The level of assessment and control shall depend on the safety significance of the task. 4.26. All activities important to safety shall be carried out in accordance with written procedures to ensure that the plant is operated within the established operational limits and conditions. Acceptable margins shall be ensured between normal operating values and the established safety system settings to avoid undesirably frequent actuation of safety systems. 4.27. No experiments shall be conducted without adequate justification. If there is a need to conduct a non-routine operation or test that is not covered by existing operating procedures, a specific safety review shall be performed and a special procedure shall be developed and subject to approval in accordance with national or other relevant regulations. 4.28. Written communication shall be preferred and spoken communication shall be minimized. If spoken communication is used, attention shall be given to ensuring that spoken instructions are clearly understood. 4.29. Aspects of the working environment that influence human performance factors (such as workload or fatigue) and the effectiveness and fitness of personnel for duty shall be identified and controlled. Tools for enhancing human performance shall be used as appropriate to support the responses of operating personnel. 4.30. The operating organization shall encourage plant personnel to have a questioning attitude and to make appropriate and conservative decisions, so as to minimize risk and to maintain the plant in a safe condition. 4.31. The responsibilities and authorities for restarting a reactor after an event leading to an unplanned shutdown, scram or major transient, or to an extended period of maintenance, shall be clearly established in writing. An investigation shall be carried out to determine the cause of the event (by means of root cause analysis wherever necessary) and corrective actions shall be taken to make its recurrence less likely. Prior to the restart or the resumption of full power of the affected plant, the operating organization shall carry out necessary remedial actions, including inspection, testing and repair of damaged structures, systems and components, and shall revalidate the safety functions that might be challenged by the event. Restart conditions and criteria shall be established and followed after the timely implementation of the necessary corrective actions. 4.32. If a probabilistic assessment of risk is to be used for decision making purposes, the operating organization shall ensure that the risk analysis is of appropriate quality and scope for decision making purposes. The risk analysis shall be performed by appropriately skilled analysts and shall be used in a manner that complements the deterministic approach to decision making, in compliance with applicable regulations and plant licence conditions.	Risks associated with safety related activities are higher than reasonably achieveable	Establishment of a risk management program that ensures that risks are identified, analyzed and reduced to levels as low as reasonably achieveable. All activities important to safety shall be carried out in accordance with written procedures to ensure that the plant is operated within the established operational limits and conditions. Written communication shall be preferred and spoken communication shall be minimized. If spoken communication is used, attention shall be given to ensuring that spoken instructions are clearly understood. Aspects of the working environment that influence human performance factors (such as workload or fatigue) and the effectiveness and fitness of personnel for duty shall be identified and controlled. The operating organization shall encourage plant personnel to have a questioning attitude and to make appropriate and conservative decisions, so as to minimize risk and to maintain the plant in a safe condition.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
86	2	Requirement 9: Monitoring and review of safety performance	The operating organization shall establish a system for continuous monitoring and periodic review of the safety of the plant and of the performance of the operating organization.	4.33. An adequate audit and review system shall be established by the operating organization to ensure that the safety policy of the operating organization is being implemented effectively and that lessons are being learned from its own experience and from the experience of others to improve safety performance. 4.34. Self-assessment by the operating organization shall be an integral part of the monitoring and review system. The operating organization shall perform systematic self-assessments to identify achievements and to address any degradation in safety performance. Where practicable, suitable objective performance indicators shall be developed and used to enable senior managers to detect and to react to shortcomings and deterioration in the management of safety. 4.35. Monitoring of safety performance shall include the monitoring of: personnel performance; attitudes to safety; response to infringements of safety; and violations of operational limits and conditions, operating procedures, regulations and licence conditions. The monitoring of plant conditions, activities and attitudes of personnel shall be supported by systematic walkdowns of the plant by the plant managers. 4.36. The persons and organization performing quality assurance functions shall have sufficient authority and organizational independence to identify problems relating to quality and to initiate, to recommend and to verify the implementation of solutions. These persons and organizations shall report to a high level of management such that the necessary authority and organizational independence are provided, including sufficient independence from costs and schedules when considering safety related matters. 4.37. The appropriate corrective actions shall be determined and implemented as a result of the monitoring and review of safety performance. Progress in taking the corrective actions shall be monitored to ensure that actions are completed within the appropriate timescales. The completed corrective actions shall be reviewed to assess whether they have adequately addressed the issues identified in audits and reviews.	Cumulative effect of changes to processes, organizations and governance result in non-compliance with safety requirements Non-compliance with the safety management program	Establish an audit and review program to ensure that the safety management program has been effectively implemented and continuously improved over time Establish the organization responsible for audit and review to have sufficient authority and organizational independence to be able to identify problems, to recommend solutions and to verify that solutions have been effectively implemented.

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
87	3	Requirement 10: Management of processes and activities	Processes and activities shall be developed and shall be effectively managed to achieve the organization's goals without compromising safety.	4.28. Each process shall be developed and shall be managed to ensure that requirements are met without compromising safety. Processes shall be documented and the necessary supporting documentation shall be maintained. It shall be ensured that process documentation is consistent with any existing documents of the organization. Records to demonstrate that the results of the respective process have been achieved shall be specified in the process documentation. 4.29. The sequencing of a process and the interactions between processes shall be specified so that safety is not compromised. Effective interaction between interfacing processes shall be ensured. Particular consideration shall be given to interactions between processes within the organization, and to interactions between processes conducted by the organization and processes conducted by external service providers. 4.30. New processes or modifications to existing processes shall be designed, verified, approved and applied so that safety is not compromised. Processes, including any subsequent modifications to them, shall be aligned with the goals, strategies, plans and objectives of the organization. 4.31. Any activities for inspection, testing, and verification and validation, their acceptance criteria and the responsibilities for carrying out such activities shall be specified. It shall be specified when and at what stages independent inspection, testing, and verification and validation are required to be conducted. 4.32. Each process or activity that could have implications for safety shall be carried out under controlled conditions, by means of following readily understood, approved and current procedures, instructions and drawings. These procedures, instructions and drawings shall be validated before their first use and shall be periodically reviewed to ensure their adequacy and effectiveness. Individuals carrying out such activities shall be involved in the validation and the periodic review of such procedures, instructions and drawings.	Safety is compromised due to the implementation of processes that have not taken safety consequences of the process into account	Effective documentation of processes that is maintained as configuration items in a configuration management program Effective review of processes to ensure that safety consequences are taken into account within each process, and in the interactions between processes

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
88	3	Requirement 13: Measurement, assessment and improvement of the management system	The effectiveness of the management system shall be measured, assessed and improved to enhance safety performance, including minimizing the occurrence of problems relating to safety.	6.1. The effectiveness of the management system shall be monitored and measured to confirm the ability of the organization to achieve the results intended and to identify opportunities for improvement of the management system. 6.2. All processes shall be regularly evaluated for their effectiveness and for their ability to ensure safety. 6.3. The causes of non-conformances of processes and the causes of safety related events that could give rise to radiation risks shall be evaluated and any consequences shall be managed and shall be mitigated. The corrective actions necessary for eliminating the causes of non-conformances, and for preventing the occurrence of, or mitigating the consequences of, similar safety related events, shall be determined, and corrective actions shall be taken in a timely manner. The status and effectiveness of all corrective actions and preventive actions taken shall be monitored and shall be reported to the management at an appropriate level in the organization. 6.4. Independent assessments and self-assessments of the management system shall be regularly conducted to evaluate its effectiveness and to identify opportunities for its improvement. Lessons and any resulting significant changes shall be analysed for their implications for safety. 6.5. Responsibility shall be assigned for conducting independent assessments of the management system. The organizations, entities (in-house or external) and individuals assigned such responsibilities shall be given sufficient authority to discharge their responsibilities and shall have direct access to senior management. In addition, individuals conducting independent assessments of the management system shall not be assigned responsibility to assess areas under the responsibility of their own line management. 6.6. Senior management shall conduct a review of the management system at planned intervals to confirm its suitability and effectiveness, and its ability to enable the objectives of the organization to be accomplished, with account taken of new requirements and changes in the organization. 6.7. The management system shall include evaluation and timely use of the following: (a) Lessons from experience gained and from events that have occurred, both within the organization and outside the organization, and lessons from identifying the causes of events; (b) Technical advances and results of research and development; (c) Lessons from identifying good practices. 6.8. Organizations shall make arrangements to learn from successes and from strengths for their organizational development and continuous improvement.	Ineffective management of the governance programs within the organization resulting in governance practices that are not effective at achieving and maintaining safety, or resulting in non-compliances with effectively defined programs.	Establishment of a set of programs necessary to achieve and maintain safety along with the establishment of an effective management system for the programs

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
89	3	Requirement 14: Measurement, assessment and improvement of leadership for safety and of safety culture	Senior management shall regularly commission assessments of leadership for safety and of safety culture in its own organization.	6.9. Senior management shall ensure that self-assessment of leadership for safety and of safety culture includes assessment at all organizational levels and for all functions in the organization. Senior management shall ensure that such self-assessment makes use of recognized experts in the assessment of leadership and of safety culture. 6.10. Senior management shall ensure that an independent assessment of leadership for safety and of safety culture is conducted for enhancement of the organizational culture for safety (i.e. the organizational culture as it relates to safety and as it fosters a strong safety culture in the organization). 6.11. The results of self-assessments and independent assessments of leadership for safety and of safety culture [1] shall be communicated at all levels in the organization. The results of such assessments shall be acted upon to foster and sustain a strong safety culture, to improve leadership for safety and to foster a learning attitude within the organization.	Non-compliance with programs that are pre-requisite to achieving and maintaining safety	Establishment of a leadership for safety program

PERFORMANCE MONITORING & CONTINUOUS IMPROVEMENT

Organizations

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
99	3	Requirement 9: Provision of resources	Senior management shall determine the competences and resources necessary to carry out the activities of the organization safely and shall provide them.	4.21. Senior management shall make arrangements to ensure that the organization has in-house, or maintains access to, the full range of competences and the resources necessary to conduct its activities and to discharge its responsibilities for ensuring safety at each stage in the lifetime of the facility or activity, and during an emergency response [13, 14, 18].10 4.22. Senior management shall determine which competences and resources the organization has to retain or has to develop internally, and which competences and resources may be obtained externally, for ensuring safety. 4.23. Senior management shall ensure that competence requirements for individuals at all levels are specified and shall ensure that training is conducted, or other actions are taken, to achieve and to sustain the required levels of competence. An evaluation shall be conducted of the effectiveness of the training and of the actions taken. 4.24. Competences to be sustained in-house by the organization shall include: competences for leadership at all management levels; competences for fostering and sustaining a strong safety culture; and expertise to understand technical, human and organizational aspects relating to the facility or the activity in order to ensure safety. 4.25. Senior management shall ensure that individuals at all levels, including managers and workers: (a) Are competent to perform their assigned tasks and to work safely and effectively; (b) Understand the standards that they are expected to apply in completing their tasks. 4.26. All individuals in the organization shall be trained in the relevant requirements of the management system. Such training shall be conducted to ensure that individuals are knowledgeable of the relevance and the importance of their activities and of how their activities contribute to ensuring safety in the achievement of the organization’s goals. 4.27. The knowledge and the information of the organization shall be managed as a resource.	Personnel involved in the design did not have the required competencies	Competencies required for each design activity are clearly defined The management system shall ensure that personnel assigned to design activities have the pre-requisite competencies to perform those activities

PERFORMANCE MONITORING & CONTINUOUS IMPROVEMENT

Governance

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
90	3	Requirement 1: Achieving the fundamental safety objective	The registrant or licensee — starting with the senior management — shall ensure that the fundamental safety objective of protecting people and the environment from harmful effects of ionizing radiation is achieved.	2.1. The registrant or licensee shall ensure that provisions are made to achieve the fundamental safety objective. 2.2. The senior management of organizations, in accordance with their accountabilities: (a) Shall ensure the safe siting, design, construction, commissioning, operation and decommissioning (or closure) of facilities [2, 9, 11–14]; (b) Shall ensure that equipment and activities meet safety standards, quality standards and management standards; (c) Shall ensure the safe management and control of all radioactive material and radiation sources that are produced, processed, used, handled, transported, stored or disposed of [5, 15]; (d) Shall ensure that managers at all levels in the organization develop and maintain an understanding of radiation risks and potential consequences, and of how to manage radiation risks relevant to their responsibilities [16]; (e) Shall ensure that provision is made for adequate resources and funding, including for the long term management and disposal of radioactive waste, as well as for decommissioning (or closure) of facilities, with due consideration given to the protection of future generations [9, 15, 17]; (f) Shall ensure that adequate arrangements are made where appropriate for preparedness and response for a nuclear or radiological emergency [18, 19].	Ineffective safety management program Non-compliance with safety management program	Establish accountabilities for senior management to establish a safety management program Establish accountabilities for senior management to effectively implement the safety management program

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
91	3	Requirement 12: Fostering a culture for safety	Individuals in the organization, from senior managers downwards, shall foster a strong safety culture. The management system and leadership for safety shall be such as to foster and sustain a strong safety culture.	5.1. All individuals in the organization shall contribute to fostering and sustaining a strong safety culture [1, 2]. 5.2. Senior managers and all other managers shall advocate and support the following: (a) A common understanding of safety and of safety culture, including: awareness of radiation risks and hazards relating to work and to the working environment; an understanding of the significance of radiation risks and hazards for safety; and a collective commitment to safety by teams and individuals; (b) Acceptance by individuals of personal accountability for their attitudes and conduct with regard to safety; (c) An organizational culture that supports and encourages trust, collaboration, consultation and communication; (d) The reporting of problems relating to technical, human and organizational factors and reporting of any deficiencies in structures, systems and components to avoid degradation of safety, including the timely acknowledgement of, and reporting back of, actions taken; (e) Measures to encourage a questioning and learning attitude at all levels in the organization and to discourage complacency with regard to safety; (f) The means by which the organization seeks to enhance safety and to foster and sustain a strong safety culture, and using a systemic approach (i.e. an approach relating to the system as a whole in which the interactions between technical, human and organizational factors are duly considered); (g) Safety oriented decision making in all activities; (h) The exchange of ideas between, and the combination of, safety culture and security culture.	Decisions impacting safety are not made consistent with a strong safety culture	Establish accountabilities for managers to support and advocate a strong safety culture

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
92	3	Requirement 2: Demonstration of leadership for safety by managers	Managers shall demonstrate leadership for safety and commitment to safety.	3.1. The senior management of the organization shall demonstrate leadership for safety by: (a) Establishing, advocating and adhering to an organizational approach to safety that stipulates that, as an overriding priority, issues relating to protection and safety receive the attention warranted by their significance; (b) Acknowledging that safety encompasses interactions between people, technology and the organization [2]; (c) Establishing behavioural expectations and fostering a strong safety culture; (d) Establishing the acceptance of personal accountability in relation to safety on the part of all individuals in the organization and establishing that decisions taken at all levels take account of the priorities and accountabilities for safety. 3.2. Managers at all levels in the organization, taking into account their duties, shall ensure that their leadership includes: (a) Setting goals for safety that are consistent with the organization's policy for safety, actively seeking information on safety performance within their area of responsibility and demonstrating commitment to improving safety performance; (b) Development of individual and institutional values and expectations for safety throughout the organization by means of their decisions, statements and actions; (c) Ensuring that their actions serve to encourage the reporting of safety related problems, to develop questioning and learning attitudes, and to correct acts or conditions that are adverse to safety. 3.3. Managers at all levels in the organization: (a) Shall encourage and support all individuals in achieving safety goals and performing their tasks safely; (b) Shall engage all individuals in enhancing safety performance; (c) Shall communicate clearly the basis for decisions relevant to safety.	Safety issues are not given the attention warranted by their significance Decisions at all levels in the organization do not take safety into account Expectations for safety related performance of personnel are not clearly established and communicated	Clearly established policy and governance with respect to the expectations for taking safety into account in all decisions Clearly established expectations on the leadership to communicate, demonstrate and reinforce the expected safety behaviour
93	3	Requirement 3: Responsibility of senior management for the management system	Senior management shall be responsible for establishing, applying, sustaining and continuously improving a management system to ensure safety.	4.1. Senior management shall retain accountability for the management system even where individuals are assigned responsibility for coordinating the development, application and maintenance of the management system [1, 2]. 4.2. Senior management shall be responsible for establishing safety policy.	Lack of an effective management system to achieve safety	Clear accountability for the establishment and implementation of a safety management system

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
94	3	Requirement 4: Goals, strategies, plans and objectives	Senior management shall establish goals, strategies, plans and objectives for the organization that are consistent with the organization's safety policy.	4.3. Goals, strategies, plans and objectives for the organization shall be developed in such a manner that safety is not compromised by other priorities. 4.4. Senior management shall ensure that measurable safety goals that are in line with these strategies, plans and objectives are established at various levels in the organization. 4.5. Senior management shall ensure that goals, strategies and plans are periodically reviewed against the safety objectives, and that actions are taken where necessary to address any deviations.	Decisions impacting safety are not given adequate priority. For example: - requirements for design process not established consistent with best practices, - staff qualifications not consistent with competencies required to perform design processes competently	Clear and measurable safety goals are established at various levels in the organizations Expectation that safety goals are periodically reviewed against organizational strategies and plans are established
95	3	Requirement 5: Interaction with interested parties	Senior management shall ensure that appropriate interaction with interested parties takes place.	4.6. Senior management shall identify interested parties for their organization and shall define an appropriate strategy for interaction with them. 4.7. Senior management shall ensure that the processes and plans resulting from the strategy for interaction with interested parties include: (a) Appropriate means of communicating routinely and effectively with and informing interested parties with regard to radiation risks associated with the operation of facilities and the conduct of activities; (b) Appropriate means of timely and effective communication with interested parties in circumstances that have changed or that were unanticipated; (c) Appropriate means of dissemination to interested parties of necessary information relevant to safety; (d) Appropriate means of considering in decision making processes the concerns and expectations of interested parties in relation to safety.	Organization's criteria for safety is not consistent with the public's perception of tolerable risk	Expectation for effective communications and interactions with interested parties about safety is established

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
96	3	Requirement 6: Integration of the management system	The management system shall integrate its elements, including safety, health, environmental, security, quality, human-and-organizational-factor, societal and economic elements, so that safety is not compromised.	4.8. The management system shall be developed, applied and continuously improved. It shall be aligned with the safety goals of the organization. 4.9. The management system shall be applied to achieve goals safely, to enhance safety and to foster a strong safety culture by: (a) Bringing together in a coherent manner all the necessary elements for safely managing the organization and its activities; (b) Describing the arrangements made for management of the organization and its activities; (c) Describing the planned and systematic actions necessary to provide confidence that all requirements are met; (d) Ensuring that safety is taken into account in decision making and is not compromised by any decisions taken. 4.10. Arrangements shall be made in the management system for the resolution of conflicts arising in decision making processes. Potential impacts of security measures on safety and potential impacts of safety measures on security shall be identified and shall be resolved without compromising safety or security [20–23]. 4.11. The organizational structures, processes, responsibilities, accountabilities, levels of authority and interfaces within the organization and with external organizations shall be clearly specified in the management system. 4.12. Regulatory requirements shall be reflected in the management system. 4.13. Provision shall be made in the management system to identify any changes (including organizational changes and the cumulative effects of minor changes) that could have significant implications for safety and to ensure that they are appropriately analysed. 4.14. Arrangements shall be established in the management system for an independent review to be made before decisions significant for safety are made. The requirements on the independent nature of the review and on the necessary competences of the reviewers shall be specified in the management system.	The management system is not aligned with the safety goals of the organizations All elements necessary to achieve safety are not well integrated into the management system resulting in safety being compromised Continuous improvement of the safety management system is not effectively implemented due to lack of identification of issues, assessment of issues and taking of effective corrective actions.	Expectations that the safety management system be developed, applied and continuously improved shall be established. The safety management system shall be integrated into the overall management system
97	3	Requirement 7: Application of the graded approach to the management system	The management system shall be developed and applied using a graded approach.	4.15. The criteria used to grade the development and application of the management system shall be documented in the management system. The following shall be taken into account: (a) The safety significance and complexity of the organization, operation of the facility or conduct of the activity; (b) The hazards and the magnitude of the potential impacts (risks) associated with the safety, health, environmental, security, quality and economic elements of each facility or activity [16, 24–26]; (c) The possible consequences for safety if a failure or an unanticipated event occurs or if an activity is inadequately planned or improperly carried out.	Lack of effective decision making relative to safety for decisions having a significant impact on safety	Criteria are established to grade the development and application of the management system taking into account the safety significance of decisions

No.	Ref	Requirement Heading	Requirement	Detailed Requirement	Cause of Hazard Addressed by Requirement	Design Feature Used to Deal with the Cause
98	3	Requirement 8: Documentation of the management system	The management system shall be documented. The documentation of the management system shall be controlled, usable, readable, clearly identified and readily available at the point of use.	4.16. The documentation of the management system shall include as a minimum: policy statements of the organization on values and behavioural expectations; the fundamental safety objective; a description of the organization and its structure; a description of the responsibilities and accountabilities; the levels of authority, including all interactions of those managing, performing and assessing work and including all processes; a description of how the management system complies with regulatory requirements that apply to the organization; and a description of the interactions with external organizations and with interested parties. 4.17. Documents shall be controlled. All individuals responsible for preparing, reviewing, revising and approving documents shall be competent to perform the tasks and shall be given access to appropriate information on which to base their input or decisions. 4.18. Revisions to documents shall be controlled, reviewed and recorded. Revised documents shall be subject to the same level of approval as the initial documents. 4.19. Records shall be specified in the management system and shall be controlled. All records shall be readable, complete, identifiable and easily retrievable. 4.20. Retention times of records and associated test materials and specimens shall be established to be consistent with the statutory requirements and with the obligations for knowledge management of the organization. The media used for records shall be such as to ensure that the records are readable for the duration of the retention times specified for each record.	Lack of clear documentation and communication of the safety management system	Establishment of clear expectations on the documentation, revisions control and communication of the safety management system

APPENDIX 4 - Recommendations to Address Causes of Fukushima Accident

This appendix lists the recommendations from eight reference reports made to avoid reoccurrence of the Fukushima accident. For each recommendation a review of the principles in Appendix 3 was performed to identify which principles should have avoided the need for the recommendation. If no principles were found, then None was entered in the Principles column of the table. Recommendations with no principles corresponding to them indicate areas of weakness in the IAEA principles.

The table is structured as follows:

No.: A unique number for each recommendation

Ref: A number indicating which reference document was the basis of the recommendation as follows:

1) Fukushima Nuclear Accident Analysis Report (TEPCO – owner of Fukushima Daiichi NPP) [48]
2) Report of the Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations (Japanese Government) [49]
3) Examination of Accident at Tokyo Electric Power Co., Inc.'s Fukushima Daiichi Nuclear Power Station and Proposal of Countermeasures. (Japan Nuclear Technology Institute) [50]
4) Executive Summary of the Final Report (Investigation Committee on the Accident at Fukushima Nuclear Power Stations of Tokyo Electric Power Company) [51]
5) The Fukushima Daiichi Accident (IAEA) [52]
6) Lessons Learned from the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station (INPO) [53]
7) CNSC Fukushima Task Force Report (CNSC) [47]
8) Lessons Learned from the Fukushima Nuclear Accident for Improving Safety of U.S. Nuclear Plants (US NRC) [1]

Area: The area within which the recommendation applies. Each report identifies areas differently, so the titles used in this column are unique to each report.

Recommendation: A summary of the recommendations made by each report

Principles: The No. of the principle in Appendix 3 that, if applied, would address the recommendation.

Design View: A letter indicating which design view to which the recommendation would mostly correspond as follows:

T – technical

P – business process

O – organization

G - governance

LC Phase: Identifies which lifecycle phases the recommendation would mostly correspond as follows:

DC – Design and Construction

OM – Operations and Maintenance

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
107	1	Facility	Thorough flooding countermeasures for buildings	None	T	DC
108	1	Facility	High pressure cooling water injection facilities	49	T	DC
109	1	Facility	Depressurization equipment	None	T	DC
110	1	Facility	Low pressure water injection systems	None	T	DC
111	1	Facility	Heat removal and cooling facilities	49 / 59	T	DC
112	1	Facility	Securing power for monitoring instruments.	None	T	DC
113	1	Facility	Measures to mitigate impact after reactor core damage	None	P	OM
114	1	Common Facility	Off-site power	49	T	DC
115	1	Common Facility	Debris removal equipment	None	T	DC
116	1	Common Facility	Securing communication methods	56	P	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
117	1	Common Facility	Securing lighting equipment	49	P	OM
118	1	Common Facility	Protective equipment	None	T	DC
119	1	Common Facility	Preparation of radiation control tools	None	P	OM
120	1	Common Facility	Reinforcement of environmental radiation monitoring organization	None	O	OM
121	1	Common Facility	Reinforcement of tsunami monitoring organization	None	O	OM
122	1	Common Facility	Enhancement of functionality for the seismic isolated building	None	T	DC
123	1	Administration	Develop concrete implementation procedures	48	P	OM
124	1	Administration	Back up with appropriate staffing and organizational structure	None	O	OM
125	1	Administration	Provide and train on skills and knowledge	209	O	OM
126	1	Administration	Emergency response organization	None	O	OM
127	1	Administration	Chain of command	None	O	OM
128	1	Administration	Establishing long-term response organization	None	O	OM
129	1	Administration	Ensure availability of initial response organization	None	O	OM
130	1	Administration	Information communication and sharing	107 / 213	G	OM
131	1	Administration	Actions for which responsible organization is not designated	None	O	OM
132	1	Administration	Information disclosure	107 / 213	G	OM
133	1	Administration	Transportation of materials and equipment	None	P	OM
134	1	Administration	Establishing an access control center	None	O	OM
135	1	Administration	Ensuring safety during nuclear disasters (radiation safety)	None	G	OM
136	1	Administration	Develop approach for female workers	None	P	OM
137	1	Administration	Develop internal exposure assessment methods and response procedures	None	P	OM
138	1	Administration	Assessment of equipment conditions and performance	None	G	OM
139	1	Other Organizations	The nature of the off-site center	None	O	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
140	1	Other Organizations	Procurement of materials and equipment	None	P	DC
141	1	Other Organizations	Method to Review Emergency Dose Limits and Screening Levels	None	P	OM
142	1	Other Organizations	Develop external event standards	155 / 159	P	OM
143	1	Other Organizations	Use of tsunami data	None	G	OM
144	1	Other Organizations	Investigation on effects of low dose exposure	None	G	OM
145	1	Other Organizations	Strengthen crisis management and prevention measures against rare but serious risks	143	G	OM
146	1	Other Organizations	Revise and strengthen promotional systems	None	O	OM
146 b	1	Risk Management	Strengthen crisis management and prevention measures against rare but serious risks	None	P	OM
146 c	1	Risk Management	Revise and strengthen promotional systems	None	O	OM
147	1	Risk Management	Foster safety awareness and climate	65 / 66 / 70 / 73 / 74 / 100 / 118 / 138 / 143 / 146 / 149 / 150 / 160 / 200	G	OM
148	1	Risk Management	Improve risk communication	120 / 135	P	OM
149	1	Risk Management	Revise risk management guidelines and risk management regulations	None	P	OM
150	2	Strengthen preventive measures against a	Strengthen measures against earthquakes and tsunamis	149 / 164 / 171 / 172 / 176 / 188	T	DC

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
		severe accident				
151	2	Strengthen preventive measures against a severe accident	Ensure power supplies	186	T	DC
152	2	Strengthen preventive measures against a severe accident	Ensure robust cooling functions of reactors and PCVs	49 / 149 / 150 / 151 / 169 / 178 / 180 / 181 / 185 / 186 / 187 / 208 / 210 / 218	T	DC
153	2	Strengthen preventive measures against a severe accident	Ensure robust cooling functions of spent fuel pools	150 / 188	T	DC
154	2	Strengthen preventive measures against a severe accident	Thorough accident management (AM) measures	48 / 49	P	OM
155	2	Strengthen preventive measures against a	Response to issues concerning the siting with more than one reactor	None	T	DC

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
		severe accident				
156	2	Strengthen preventive measures against a severe accident	Consideration of NPS arrangement in basic designs	None	T	DC
157	2	Strengthen preventive measures against a severe accident	Ensuring the water tightness of essential equipment facilities	None	T	DC
158	2	Enhancement of response measures against severe accidents	Enhancement of measures to prevent hydrogen explosions	None	T	DC
159	2	Enhancement of response measures against severe accidents	Enhancement of containment venting system	None	T	DC
160	2	Enhancement of response measures against severe accidents	Improvements to the accident response environment	None	O	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
161	2	Enhancement of response measures against severe accidents	Enhancement of the radiation exposure management system at the time of the accident	145 / 203	P	OM
162	2	Enhancement of response measures against severe accidents	Enhancement of training responding to severe accidents	209	O	OM
163	2	Enhancement of response measures against severe accidents	Enhancement of instrumentation to identify the status of the reactors and PCVs	None	T	DC
164	2	Enhancement of response measures against severe accidents	Central control of emergency supplies and equipment and setting up rescue teams	None	P	OM
165	2	Enhancement of nuclear emergency responses	Responses to combined emergencies of both large-scale natural disasters and prolonged nuclear accident	None	P	OM
166	2	Enhancement of nuclear emergency responses	Reinforcement of environmental monitoring	None	T	DC
167	2	Enhancement of nuclear emergency responses	Establishment of a clear division of labor between relevant central and local organizations	None	O	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
168	2	Enhancement of nuclear emergency responses	Enhancement of communication relevant to the accident	107 / 208	G	OM
169	2	Enhancement of nuclear emergency responses	Enhancement of responses to assistance from other countries and communication to the international community	110	G	OM
170	2	Enhancement of nuclear emergency responses	Adequate identification and forecasting of the effect of released radioactive materials	None	P	OM
171	2	Enhancement of nuclear emergency responses	Clear definition of widespread evacuation areas and radiological protection guidelines in nuclear emergency	None	P	OM
172	2	Reinforcement of safety infrastructure	Reinforcement of safety regulatory bodies	None	O	OM
173	2	Reinforcement of safety infrastructure	Establishment and reinforcement of legal structures, criteria and guidelines	115	O	OM
174	2	Reinforcement of safety infrastructure	Human resources for nuclear safety and nuclear emergency preparedness and responses	None	O	OM
175	2	Reinforcement of safety infrastructure	Ensuring the independence and diversity of safety systems	14 / 143 / 150 / 171 / 217	T	DC
176	2	Reinforcement of safety infrastructure	Effective use of probabilistic safety assessment (PSA) in risk management	6	P	DC

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
177	2	Thoroughly instill a safety culture	Thoroughly instill a safety culture	65 / 66 / 70 / 73 / 74 / 100 / 118 / 138 / 143 / 146 / 149 / 150 / 160 / 200	G	OM
1	3	Countermeasures against natural hazards	Countermeasures against natural hazards	22 / 161 / 171	T	DC
2	3	Preparation of Power Sources	Preparation of Power Sources	None	T	DC
3	3	Measures against loss of heat sink systems	Measures against loss of heat sink systems	164 / 208	T	DC
4	3	Measures against hydrogen leakage	Measures against hydrogen leakage	None	T	DC
5	3	Preparation for emergencies (training and drills)	Preparation for emergencies (training and drills)	209	O	OM
221	4	Countermeasures against natural hazards	Countermeasures against natural hazards	22 / 161 / 171	T	DC
222	4	Securing of power supply	Securing of power supply	None	T	DC

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
223	4	Measures against loss of heat sink systems	Measures against loss of heat sink systems	164 / 208	T	DC
224	4	Measures against hydrogen leakage	Measures against hydrogen leakage	None	T	DC
225	4	Preparation for emergencies (training and drills)	Preparation for emergencies (training and drills)	209	O	OM
400	4	safety measures and emergency preparedness	Recommendations for emergency preparedness in light of complex disasters in mind	None	P	OM
401	4	safety measures and emergency preparedness	Recommendations for changing an attitude to face risks	None	G	OM
402	4	safety measures and emergency preparedness	Recommendations for “deficiency analysis from the disaster victims’ standpoint"	None	P	OM
403	4	safety measures and emergency preparedness	Recommendations for incorporating the latest knowledge in the emergency preparedness	None	P	OM
404	4	safety measures regarding	Recommendations for building disaster preventive measures	None	T	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
		nuclear power generation				
405	4	safety measures regarding nuclear power generation	Recommendations for the necessity of comprehensive risk analysis	None	G	OM
406	4	safety measures regarding nuclear power generation	Recommendations for severe accident management	None	P	OM
407	4	nuclear emergency response systems	Recommendations for reforming the crisis management system for a nuclear emergency	None	P	OM
408	4	nuclear emergency response systems	Recommendations for the nuclear emergency response headquarters	None	O	OM
409	4	nuclear emergency response systems	Recommendations for off-site centers	None	O	OM
410	4	nuclear emergency response systems	Recommendations for the roles of the prefectural government in nuclear emergency responses	None	O	OM
411	4	damage prevention and mitigation	Recommendations for the provision of information and risk communication	None	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
412	4	damage prevention and mitigation	Recommendations for improving radiation monitoring operations	None	P	OM
413	4	damage prevention and mitigation	Recommendations for the SPEEDI system	None	P	OM
414	4	damage prevention and mitigation	Recommendations for evacuation procedures of residents	None	P	OM
415	4	damage prevention and mitigation	Recommendations for the intake of stable iodine tablets	None	P	OM
416	4	damage prevention and mitigation	Recommendations for radiation emergency medical care institutions	None	O	OM
417	4	damage prevention and mitigation	Recommendations for public understanding of radiation effects	None	P	OM
418	4	damage prevention and mitigation	Recommendations for information sharing with, and receiving support from, overseas	None	P	OM
419	4	harmonization with international practices	Recommendations for harmonization with international practices such as IAEA safety standards	None	P	OM
420	4	relevant organizations	Recommendations for the nuclear safety regulating body	None	P	OM
421	4	relevant organizations	Recommendations for TEPCO	None	P	OM
422	4	relevant organizations	Recommendations for rebuilding a safety culture	None	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
423	4	continued investigation of accident causes and damage	Recommendations for continued investigation of accident cause	None	P	OM
424	4	continued investigation of accident causes and damage	Recommendations for extended investigation of the whole picture of accident damage	None	P	OM
6	5	Nuclear Safety	The assessment of natural hazards needs to be sufficiently conservative. The consideration of mainly historical data in the establishment of the design basis of NPPs is not sufficient to characterize the risks of extreme natural hazards. Even when comprehensive data are available, due to the relatively short observation periods, large uncertainties remain in the prediction of natural hazards.	167 / 175	G	DC
7	5	Nuclear Safety	The safety of NPPs needs to be re-evaluated on a periodic basis to consider advances in knowledge, and necessary corrective actions or compensatory measures need to be implemented promptly.	114 / 154 / 159	P	OM
8	5	Nuclear Safety	The assessment of natural hazards needs to consider the potential for their occurrence in combination, either simultaneously or sequentially, and their combined effects on an NPP. The assessment of natural hazards also needs to consider their effects on multiple units at an NPP.	None	P	OM
9	5	Nuclear Safety	Operating experience programmes need to include experience from both national and international sources. Safety improvements identified through operating experience programmes need to be implemented promptly. The use of operating experience needs to be evaluated periodically and independently.	114 / 154 / 159	P	OM
10	5	Nuclear Safety	The defence in depth concept remains valid, but implementation of the concept needs to be strengthened at all levels by adequate independence, redundancy, diversity and protection against internal and external hazards.	None	T	DC

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
			There is a need to focus not only on accident prevention, but also on improving mitigation measures.			
11	5	Nuclear Safety	Instrumentation and control systems that are necessary during beyond design basis accidents need to remain operable in order to monitor essential plant safety parameters and to facilitate plant operations.	None	T	DC
12	5	Nuclear Safety	Robust and reliable cooling systems that can function for both design basis and beyond design basis conditions need to be provided for the removal of residual heat.	None	T	DC
13	5	Nuclear Safety	There is a need to ensure a reliable confinement function for beyond design basis accidents to prevent significant release of radioactive material to the environment.	None	T	DC
14	5	Nuclear Safety	Comprehensive probabilistic and deterministic safety analyses need to be performed to confirm the capability of a plant to withstand applicable beyond design basis accidents and to provide a high degree of confidence in the robustness of the plant design.	24	P	DC
15	5	Nuclear Safety	Accident management provisions need to be comprehensive, well designed and up to date. They need to be derived on the basis of a comprehensive set of initiating events and plant conditions and also need to provide for accidents that affect several units at a multi-unit plant.	None	T	DC
16	5	Nuclear Safety	Training, exercises and drills need to include postulated severe accident conditions to ensure that operators are as well prepared as possible. They need to include the simulated use of actual equipment that would be deployed in the management of a severe accident.	209	O	OM
17	5	Nuclear Safety	In order to ensure effective regulatory oversight of the safety of nuclear installations, it is essential that the regulatory body is independent and possesses legal authority, technical competence and a strong safety culture.	103 / 116 / 117 / 122 / 137	O	OM
18	5	Nuclear Safety	In order to promote and strengthen safety culture, individuals and organizations need to continuously challenge or re-examine the prevailing	140 / 143 / 146	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
			assumptions about nuclear safety and the implications of decisions and actions that could affect nuclear safety.			
19	5	Nuclear Safety	A systemic approach to safety needs to consider the interactions between human, organizational and technical factors. This approach needs to be taken through the entire life cycle of nuclear installations.	153	P	OM
20	5	Emergency Preparedness and Response	In preparing for the response to a possible nuclear emergency, it is necessary to consider emergencies that could involve severe damage to nuclear fuel in the reactor core or to spent fuel on the site, including those involving several units at a multi-unit plant possibly occurring at the same time as a natural disaster.	48 / 49 / 202	P	OM
21	5	Emergency Preparedness and Response	The emergency management system for response to a nuclear emergency needs to include clearly defined roles and responsibilities for the operating organization and for local and national authorities. The system, including the interactions between the operating organization and the authorities, needs to be regularly tested in exercises.	48 / 49 / 144	P	OM
22	5	Emergency Preparedness and Response	Emergency workers need to be designated, assigned clearly specified duties, regardless of which organization they work for, be given adequate training, and be properly protected during an emergency. Arrangements need to be in place to integrate into the response those emergency workers who had not been designated prior to the emergency, and helpers who volunteer to assist in the emergency response.	209	O	OM
23	5	Emergency Preparedness and Response	Arrangements need to be in place to allow decisions to be made on the implementation of predetermined urgent protective actions for the public, based on predefined plant conditions.	151 / 208 / 210 / 212 / 213	G	OM
24	5	Emergency Preparedness and Response	Arrangements need to be in place to enable urgent protective actions to be extended or modified in response to developing plant conditions or monitoring results. Arrangements are also needed to enable early protective actions to be initiated on the basis of monitoring results.	151 / 210 / 213	G	OM
25	5	Emergency Preparedness and Response	Arrangements need to be in place to ensure that protective actions and other response actions in a nuclear emergency do more good than harm. A	None	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
			comprehensive approach to decision making needs to be in place to ensure that this balance is achieved.			
26	5	Emergency Preparedness and Response	Arrangements need to be in place to assist decision makers, the public and others (e.g. medical staff) to gain an understanding of radiological health hazards in a nuclear emergency in order to make informed decisions on protective actions. Arrangements also need to be in place to address public concerns locally, nationally and internationally.	142	G	OM
27	5	Emergency Preparedness and Response	Arrangements need to be developed at the preparedness stage for termination of protective actions and other response actions, and for transition to the recovery phase.	202	P	OM
28	5	Emergency Preparedness and Response	Timely analysis of an emergency and the response to it, drawing lessons and identifying possible improvements, enhances emergency arrangements.	74 / 146 / 151	G	OM
29	5	Emergency Preparedness and Response	The implementation of international arrangements for notification and assistance needs to be strengthened.	108 / 113 / 135	P	OM
30	5	Emergency Preparedness and Response	There is a need to improve consultation and sharing of information among States on protective actions and other response actions.	113 / 114 / 159	P	OM
31	5	Radiological Consequences	In case of an accidental release of radioactive substances to the environment, the prompt quantification and characterization of the amount and composition of the release is needed. For significant releases, a comprehensive and coordinated programme of long term environmental monitoring is necessary to determine the nature and extent of the radiological impact on the environment at the local, regional and global levels.	145 / 203	P	OM
32	5	Radiological Consequences	Relevant international bodies need to develop explanations of the principles and criteria for radiation protection that are understandable for non-specialists in order to make their application clearer for decision makers and the public. As some protracted protection measures were disruptive for the affected people, a better communication strategy is	107 / 212	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
			needed to convey the justification for such measures and actions to all stakeholders, including the public.			
33	5	Radiological Consequences	Conservative decisions related to specific activity and activity concentrations in consumer products and deposition activity led to extended restrictions and associated difficulties. In a prolonged exposure situation, consistency among international standards, and between international and national standards, is beneficial, particularly those associated with drinking water, food, non-edible consumer products and deposition activity on land.	None	G	OM
34	5	Radiological Consequences	Personal radiation monitoring of representative groups of members of the public provides invaluable information for reliable estimates of radiation doses and needs to be used together with environmental measurements and appropriate dose estimation models for assessing public dose.	None	P	OM
35	5	Radiological Consequences	While dairy products were not the main pathway for the ingestion of radioiodine in Japan, it is clear that the most important method of limiting thyroid doses, especially to children, is to restrict the consumption of fresh milk from grazing cows.	151	G	OM
36	5	Radiological Consequences	A robust system is necessary for monitoring and recording occupational radiation doses, via all relevant pathways, particularly those due to internal exposure that may be incurred by workers during severe accident management activities. It is essential that suitable and sufficient personal protective equipment be available for limiting the exposure of workers during emergency response activities and that workers be sufficiently trained in its use.	51 / 134	P	OM
37	5	Radiological Consequences	The risks of radiation exposure and the attribution of health effects to radiation need to be clearly presented to stakeholders, making it unambiguous that any increases in the occurrence of health effects in populations are not attributable to exposure to radiation if levels of exposure are similar to the global average background levels of radiation.	None	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
38	5	Radiological Consequences	After a nuclear accident, health surveys are very important and useful, but should not be interpreted as epidemiological studies. The results of such health surveys are intended to provide information to support medical assistance to the affected population.	None	G	OM
39	5	Radiological Consequences	There is a need for radiological protection guidance to address the psychological consequences to members of the affected populations in the aftermath of radiological accidents. A Task Group of the ICRP has recommended that “strategies for mitigating the serious psychological consequences arising from radiological accidents be sought”	None	P	OM
40	5	Radiological Consequences	Factual information on radiation effects needs to be communicated in an understandable and timely manner to individuals in affected areas in order to enhance their understanding of protection strategies, to alleviate their concerns and support their own protection initiatives.	142	G	OM
41	5	Radiological Consequences	During any emergency phase, the focus has to be on protecting people. Doses to the biota cannot be controlled and could be potentially significant on an individual basis. Knowledge of the impacts of radiation exposure on non-human biota needs to be strengthened by improving the assessment methodology and understanding of radiation induced effects on biota populations and ecosystems. Following a large release of radionuclides to the environment, an integrated perspective needs to be adopted to ensure sustainability of agriculture, forestry, fishery and tourism, and of the use of natural resources.	142	G	OM
42	5	Post-Accident Recovery	Pre-accident planning for post-accident recovery is necessary to improve decision making under pressure in the immediate post-accident situation. National strategies and measures for post-accident recovery need to be prepared in advance in order to enable an effective and appropriate overall recovery programme to be put in place in case of a nuclear accident. These strategies and measures need to include the establishment of a legal and regulatory framework; generic remediation strategies and criteria for residual radiation doses and contamination levels; a plan for stabilization and decommissioning of damaged nuclear facilities; and a generic strategy	None	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
			for managing large quantities of contaminated material and radioactive waste.			
43	5	Post-Accident Recovery	Remediation strategies need to take account of the effectiveness and feasibility of individual measures and the amount of contaminated material that will be generated in the remediation process.	None	G	OM
44	5	Post-Accident Recovery	As part of the remediation strategy, the implementation of rigorous testing of and controls on food is necessary to prevent or minimize ingestion doses.	None	P	OM
45	5	Post-Accident Recovery	Further international guidance is needed on the practical application of safety standards for radiation protection in post-accident recovery situations.	None	G	OM
46	5	Post-Accident Recovery	Following an accident, a strategic plan for maintaining long term stable conditions and for the decommissioning of accident damaged facilities is essential for on-site recovery. The plan needs to be flexible and readily adaptable to changing conditions and new information.	49 / 202	P	OM
47	5	Post-Accident Recovery	Retrieving damaged fuel and characterizing and removing fuel debris require solutions that are specific to the accident, and special methods and tools may need to be developed.	None	P	OM
48	5	Post-Accident Recovery	National strategies and measures for post-accident recovery need to include the development of a generic strategy for managing contaminated liquid and solid material and radioactive waste, supported by generic safety assessments for discharge, storage and disposal.	None	P	OM
49	5	Post-Accident Recovery	It is necessary to recognize the socioeconomic consequences of any nuclear accident and of the subsequent protective actions, and to develop revitalization and reconstruction projects that address issues such as reconstruction of infrastructure, community revitalization and compensation.	None	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
50	5	Post-Accident Recovery	Support by stakeholders is essential for all aspects of post-accident recovery. In particular, engagement of the affected population in the decision making processes is necessary for the success, acceptability and effectiveness of the recovery and for the revitalization of communities. An effective recovery programme requires the trust and the involvement of the affected population. Confidence in the implementation of recovery measures has to be built through processes of dialogue, the provision of consistent, clear and timely information, and support to the affected population.	None	P	OM
51	6	Prepare for the Unexpected	When periodic reviews or new information indicates the potential for conditions that could significantly reduce safety margins or exceed current design assumptions, a timely, formal, and comprehensive assessment of the potential for substantial consequences should be conducted. An independent, cross-functional safety review with a plant walkdown should also be conducted to fully understand the nuclear safety implications. If the consequences could include common-mode failures of important safety systems, compensatory actions or countermeasures must be established without delay.	68 / 73 / 74 / 140	G	OM
52	6	Prepare for the Unexpected	Plant design features and operating procedures alone cannot completely mitigate the risk posed by a beyond-design-basis event. Additional preparations must be made to respond if such an event were to occur.	151 / 210 / 208	G	OM
53	6	Prepare for the Unexpected	Corporate enterprise risk management processes should consider the risks associated with low-probability, high-consequence events that could lead to core damage and spread radioactive contamination outside the plant.	None	P	OM
54	6	Operational Response	Ensure that, as the highest priority, core cooling status is clearly understood and that changes are controlled to ensure continuity of core cooling is maintained. If core cooling is uncertain, direct and timely action should be taken to establish conditions such that core cooling can be ensured.	149 / 150 / 151 / 208 / 210	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
55	6	Operational Response	Early in the response to an event, clear strategies for core cooling and recovery actions should be developed and communicated to control room and ERC personnel. In addition, leaders should establish clear priorities and provide direction and oversight to enable the strategy to be implemented effectively.	107 / 208	G	OM
56	6	Operational Response	Emergency and accident procedures should provide guidance to vent containment to maintain integrity, purge hydrogen, and support injection with low-pressure systems. Procedures should also provide guidance for performing venting under conditions such as loss of power and high radiation levels and high temperatures in areas where vent valves are located.	None	P	OM
57	6	Accident Response	Nuclear operators must establish the necessary infrastructure to respond effectively to severe accident conditions, mitigate core damage, and stabilize the units if core damage does occur. This infrastructure includes necessary personnel, equipment, training, and supporting procedures to respond to events that may affect multiple units, last for extended periods, and be initiated by beyond-design-basis events. Provisions should also be made to allow an effective corporate and industry response in support of the affected nuclear operating organization.	209	O	OM
58	6	Accident Response	Establish strategies for staffing operating crews, other key plant positions, and site and corporate emergency response organizations quickly in the initial stages of a multi-unit event and over the long duration of the event response.	None	O	OM
59	6	Accident Response	Establish contingency plans, training, and guidance to help personnel cope with the emotional concerns that can impact decision-making and reduce personnel effectiveness during a natural disaster or nuclear accident.	None	G	OM
60	6	Accident Response	Ensure primary and alternative methods for monitoring critical plant parameters and emergency response functions are available. Use drills and exercises to ensure emergency response personnel are able to use the available monitoring tools and methods.	None	O	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
61	6	Accident Response	On-site and off-site facilities necessary for coordinating emergency response activities should be designed and equipped to remain functional in the event of a natural disaster and/or a nuclear emergency.	None	T	DC
62	6	Accident Response	Ensure those who possess the expertise to operate specialized accident response equipment are available and are prepared to respond to a severe accident. This may be accomplished through contracts or by training and qualifying members of the station emergency response staff to perform these functions.	209	O	OM
63	6	Accident Response	Clearly define and communicate the roles and responsibilities of emergency response personnel to help ensure effective post-accident communications and decision-making.	None	O	OM
64	6	Accident Response	Communication methods and equipment should support accurate and timely information exchange, consistent and clear communications with the public, and information-sharing between the utility and the government.	107 / 213	G	OM
65	6	Accident Response	Radiation protection (RP) personnel must have established procedures, equipment, and staffing to support emergency response actions.	None	O	OM
66	6	Accident Response	Station emergency response plans should allow for prompt RP support of operator actions needed to establish or maintain safe shutdown and should include the needed flexibility to support such actions.	48 / 49 / 202	P	OM
67	6	Accident Response	Dose limits should allow some flexibility such that required actions can be performed during accident situations. In addition, workers should be trained or briefed on the relative risk of higher acute radiation doses.	141 / 214	G	OM
68	6	Accident Response	Off-site resources and support should be provided on a priority basis following significant events such a loss of off-site power. Emergency response plans and other corporate guiding documents should clearly state that the needs of nuclear stations are to be given highest priority in the event of an emergency situation.	151 / 213	G	OM
69	6	Design and Equipment	Equipment required to respond to a long-term loss of all AC and DC power and loss of the ultimate heat sink should be conveniently staged, protected, and maintained such that it is always ready for use if needed.	None	T	DC

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
70	6	Design and Equipment	Plant modifications may be needed to ensure critical safety functions can be maintained during a multi-unit event that involves extended loss of AC power, DC power, and the ultimate heat sink.	None	T	DC
71	6	Procedures	Optimum accident management strategies and associated implementing procedures (such as emergency operating procedures and accident management guidelines) should be developed through communications, engagement, and exchange of information among nuclear power plant operating organizations and reactor vendors. Decisions to deviate from these strategies and procedures should be made only after rigorous technical and independent safety reviews that consider the basis of the original standard and the potential unintended consequences.	208	G	OM
72	6	Procedures	Conditions during and following a natural disaster or an internal plant event may significantly impede and delay the ability of plant operators and others to respond and take needed actions. The potential for such delays should be considered when procedures and plans for time-sensitive operator actions are being established.	None	P	OM
73	6	Knowledge and Skills	On-shift personnel and on- and off-site emergency responders need to have in-depth accident management knowledge and skills to respond to severe accidents effectively. Training materials should be developed and training should be implemented using the systematic approach to training.	209	O	OM
74	6	Operating Experience	Actively participate and make best use of operating experience information shared in international organizations and forums.	74 / 75 / 138 / 160 / 205	G	OM
75	6	Operating Experience	When considering the applicability of significant operating experience from international events, go beyond the event causes and transient initiators and consider the potential to experience the same consequences through other means. Take timely action to strengthen defenses to such vulnerabilities.	205	G	OM
76	6	Nuclear Safety Culture	Behaviors prior to and during the Fukushima Daiichi event revealed the need to strengthen several aspects of nuclear safety culture. It would be beneficial for all nuclear operating organizations to examine their own practices and behaviors in light of this event and use case studies or other	65 / 66 / 70 / 73 / 74 / 100 / 118 / 138 / 143 / 146 / 149 / 150 / 160 / 200	G	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
			approaches to heighten awareness of safety culture principles and attributes.			
80	7	consideration of beyond-design-basis accidents	a major class of beyond design basis accidents involve loss of all heat sinks; assess scenario of loss of all heat sinks; assume failure of all mitigating measures to be able to identify possible mitigating strategies;	None	P	DC
81	7	consideration of beyond-design-basis accidents	requirement to install passive autocatalytic recombiners to improve mitigation of risks from hydrogen explosions	None	T	DC
82	7	consideration of beyond-design-basis accidents	look to extend the duration of backup power services	None	T	DC
83	7	consideration of beyond-design-basis accidents	assess survivability of instrumentation required for accident management actions	None	T	DC
900	7	Strengthening Reactor Defence in Depth	containment performance to prevent unfiltered releases of radioactive products	None	T	DC
901	7	Strengthening Reactor Defence in Depth	control capabilities for hydrogen and other combustible gases	None	T	DC
902	7	Strengthening Reactor Defence in Depth	adequacy and survivability of equipment and instrumentation	None	T	DC

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
903	7	Enhancing Emergency Response	upgrading onsite emergency facilities and equipment	None	T	DC
904	7	Enhancing Emergency Response	Strengthen federal and provincial emergency planning	None	P	OM
905	7	Improved Regulatory Framework and Licensing	require licensees to submit offsite emergency plans	None	P	OM
906	7	Improved Regulatory Framework and Licensing	describe regulatory requirements during the phases of an emergency in greater detail	None	P	OM
907	7	Improved Regulatory Framework and Licensing	periodic safety reviews	None	P	OM
226	8	Plant Operations and Safety Regulations	FINDING 5.1: Nuclear plant operators and regulators in the United States and other countries have identified and are taking useful actions to upgrade nuclear plant systems, operating procedures, and operator training in response to the Fukushima Daiichi accident. In the United States, these actions include the nuclear industry's FLEX (diverse and flexible coping strategies) initiative as well as regulatory changes proposed by the U.S. Nuclear Regulatory Commission's Near-Term Task Force. Implementation of these actions is still under way; consequently, it is too soon to evaluate their comprehensiveness, effectiveness, or status in the regulatory framework.	None	O	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
227	8	Plant Operations and Safety Regulations	FINDING 5.2: Beyond-design-basis events—particularly low-frequency, high-magnitude (i.e., extreme) events—can produce severe accidents at nuclear plants that damage reactor cores and stored spent fuel. Such accidents can result in the generation and combustion of hydrogen within the plant and release of radioactive material to the offsite environment. There is a need to better understand the safety risks that arise from such events and take appropriate countermeasures to reduce them.	None	P	DC
228	8	Plant Operations and Safety Regulations	FINDING 5.3: Four decades of analysis and operating experience have demonstrated that nuclear plant core-damage risks are dominated by beyond-design-basis accidents. Such accidents can arise, for example, from multiple human and equipment failures, violations of operational protocols, and extreme external events. Current approaches for regulating nuclear plant safety, which traditionally have been based on deterministic concepts such as the design-basis accident, are clearly inadequate for preventing core-melt accidents and mitigating their consequences. Modern risk assessment principles are beginning to be applied in nuclear reactor licensing and regulation. The more complete application of these principles in licensing and regulation could help to further reduce core-melt risks and their consequences and enhance the overall safety of all nuclear plants, especially currently operating plants.	None	P	DC
229	8	Offsite Emergency Management	FINDING 6.1: The Fukushima Daiichi accident revealed vulnerabilities in Japan's offsite emergency management. The competing demands of the earthquake and tsunami diminished the available response capacity for the accident. Implementation of existing nuclear emergency plans was overwhelmed by the extreme natural events that affected large regions, producing widespread disruption of communications, electrical power, and other critical infrastructure over an extended period of time.	None	P	OM
230	8	Offsite Emergency Management	FINDING 6.2: The committee did not have the time or resources to perform an in-depth examination of U.S. preparedness for severe nuclear accidents. Nevertheless, the accident raises the question of whether a severe nuclear accident such as occurred at the Fukushima Daiichi plant would challenge U.S. emergency response capabilities because of its severity, duration, and	None	O	OM

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
			association with a regional-scale natural disaster. The natural disaster damaged critical infrastructure and diverted emergency response resources.			
231	8	Nuclear Safety Culture	FINDING 7.1: While the Government of Japan acknowledged the need for a strong nuclear safety culture prior to the Fukushima Daiichi accident, TEPCO and its nuclear regulators were deficient in establishing, implementing, and maintaining such a culture. Examinations of the Japanese nuclear regulatory system following the Fukushima Daiichi accident concluded that regulatory agencies were not independent and were subject to regulatory capture.	148	G	OM
232	8	Nuclear Safety Culture	FINDING 7.2: The establishment, implementation, maintenance, and communication of a nuclear safety culture in the United States are priorities for the U.S. nuclear power industry and the U.S. Nuclear Regulatory Commission. The U.S. nuclear industry, acting through the Institute of Nuclear Power Operations, has voluntarily established nuclear safety culture programs and mechanisms for evaluating their implementation at nuclear plants. The U.S. Nuclear Regulatory Commission has published a policy statement on nuclear safety culture, but that statement does not contain implementation steps or specific requirements for industry adoption.	100	G	OM
233	8	Contributors to Severity of the Accident	1. Failure of the plant owner (Tokyo Electric Power Company) and the principal regulator (Nuclear and Industrial Safety Agency) to protect critical safety equipment at the plant from flooding in spite of mounting evidence that the plant's current design basis for tsunamis was inadequate.	163 / 170	G	DC
234	8	Contributors to Severity of the Accident	2. The loss of nearly all onsite AC and DC power at the plant— with the consequent loss of real-time information for monitoring critical thermodynamic parameters in reactors, containments, and spent fuel pools and for sensing and actuating critical valves and equipment— greatly narrowed options for responding to the accident.	None	T	DC

No.	Ref	Area	Recommendation	Principles	Design View	LC Phase
235	8	Contributors to Severity of the Accident	3. As a result of (1) and (2), the Unit 1, 2 and 3 reactors were effectively isolated from their ultimate heat sink (the Pacific Ocean) for a period of time far in excess of the heat capacity of the suppression pools or the coping time of the plant to station blackout.	None	T	DC
236	8	Contributors to Severity of the Accident	4. Multiunit interactions complicated the accident response. Unit operators competed for physical resources and the attention and services of staff in the onsite emergency response center.	None	O	OM
237	8	Contributors to Severity of the Accident	5. Operators and onsite emergency response center staff lacked adequate procedures and training for accidents involving extended loss of all onsite AC and DC power, particularly procedures and training for managing water levels and pressures in reactors and their containments and hydrogen generated during reactor core degradation.	209	O	OM
238	8	Contributors to Severity of the Accident	6. Failures to transmit information and instructions in an accurate and timely manner hindered responses to the accident. These failures resulted partly from the loss of communications systems and the challenging operating environments throughout the plant.	107 / 208	G	OM
239	8	Contributors to Severity of the Accident	7. The lack of clarity of roles and responsibilities within the onsite emergency response center and between the onsite and headquarters emergency response centers may have contributed to response delays.	None	O	OM
240	8	Contributors to Severity of the Accident	8. Staffing levels at the plant were inadequate for managing the accident because of its scope (affecting several reactor units) and long duration.	None	O	OM

APPENDIX 5 – Changes to IAEA Best Practice Documents After Fukushima

Changes to Documents

The following table shows specific requirements that changed in the latest version of the following two reference documents:

1. International Atomic Energy Agency. 2016. *Safety of Nuclear Power Plants: Design.*
2. International Atomic Energy Agency. 2016. *Safety of Nuclear Power Plants: Commissioning and Operation*

The preface of the two documents identify which detailed requirements have changed. The table in this appendix lists, for each changed detailed requirement, the old requirements, the new requirement and then comments on the nature of the changes made. The detailed requirements are grouped by their corresponding higher level requirement.

Ref	Section	Old Requirements	Revised Requirement	Comment
THE CONCEPT OF DEFENCE IN DEPTH				
1	2.13	2.13. Application of the concept of defence in depth in the design of a nuclear power plant provides several levels of defence (inherent features, equipment and procedures) aimed at preventing harmful effects of radiation on people and the environment, and ensuring adequate protection from harmful effects and mitigation of the consequences in the event that prevention fails. The independent effectiveness of each of the different levels of defence is an essential element of defence in depth at the plant and this is achieved by incorporating measures to	Paragraph 3.31 of the Fundamental Safety Principles [1] states that: "Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available.... The independent effectiveness of the different levels of defence is a necessary element of defence in depth." There are five levels of defence:	- minor differences

Ref	Section	Old Requirements	Revised Requirement	Comment
		avoid the failure of one level of defence causing the failure of other levels. There are five levels of defence: …		
Requirement 7: Application of defence in depth				
1	4.13A		4.13A. The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems.	- greater emphasis on independence between levels especially when considering design extension conditions
Requirement 17: Internal and external hazards				
1	Req 17	All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.	All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.	Added "in designing the layout of the plant" in last sentence

Ref	Section	Old Requirements	Revised Requirement	Comment
1	5.15A		5.15A. Items important to safety shall be designed and located, with due consideration of other implications for safety, to withstand the effects of hazards or to be protected, in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by hazards.	- strengthening defence in depth
1	5.15B		5.15B. For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously.	- multi-unit impacts taken into account

Ref	Section	Old Requirements	Revised Requirement	Comment
1	5.17	5.17. The design shall include due consideration of those natural and human induced external events (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Natural external events shall be addressed, including meteorological, hydrological, geological and seismic events. Human induced external events arising from nearby industries and transport routes shall be addressed. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and fire fighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.	5.17. The design shall include due consideration of those natural and human induced external events11 (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and firefighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.	- generalization of requirements for postulated hazards
1	5.18	5.18. Items important to safety shall be designed and located to minimize, consistent with other safety requirements, the likelihood of external events and their possible harmful consequences.	5.18. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15A.	- see 5.15 A

Ref	Section	Old Requirements	Revised Requirement	Comment
1	5.20	5.20. The design shall be such as to ensure that items important to safety are capable of withstanding the effects of external events considered in the design, and if not, other features such as passive barriers shall be provided to protect the plant and to ensure that the required safety function will be performed.	5.20. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15A.	- see 5.15 A
1	5.21	5.21. The seismic design of the plant shall provide for a sufficient safety margin to protect against seismic events and to avoid cliff edge effects (see footnote 5).	5.21. The design of the plant shall provide for an adequate margin to protect items important to safety against levels of external hazards to be considered for design, derived from the hazard evaluation for the site, and to avoid cliff edge effects.12	- focus on protecting items important to safety
	5.21A		5.21A. The design of the plant shall also provide for an adequate margin to protect items ultimately necessary to prevent an early radioactive release or a large radioactive release in the event of levels of natural hazards exceeding those considered for design, derived from the hazard evaluation for the site.	- focus on protecting items important to safety
1	5.22	5.22. For multiple unit plant sites, the design shall take due account of the potential for specific hazards giving rise to simultaneous impacts on several units on the site.	5.22. This paragraph was deleted and its content, with a broader scope, has been transferred to the new paragraph 5.15B.	- see 5.15B

Ref	Section	Old Requirements	Revised Requirement	Comment
Requirement 19: Design basis accidents				
1	Req 19	A set of accident conditions that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.	A set of accidents that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.	- Accident versus accident conditions
Requirement 20: Design extension conditions				
1	5.27	5.27. An analysis of design extension conditions for the plant shall be performed8. The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of radioactive material in the containment (including radioactive material resulting	5.27. An analysis of design extension conditions for the plant shall be performed.13 The main technical objective of considering the design extension conditions is to provide assurance that the design of the plant is such as to prevent accident conditions that are not considered design basis accident conditions, or to mitigate their consequences, as far as is reasonably practicable. This might require additional safety features for design extension conditions, or extension of the capability of safety systems to prevent, or to mitigate the consequences of, a severe accident, or to maintain the integrity of the containment. These additional safety features for design extension conditions, or this extension of the capability of safety systems, shall be such as to ensure the capability for managing accident conditions in which there is a significant amount of	- additional focus on preventing or mitigating the consequences of a severe accident

Ref	Section	Old Requirements	Revised Requirement	Comment
		from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that significant radioactive releases would be practically eliminated (see footnote 1). The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.	radioactive material in the containment (including radioactive material resulting from severe degradation of the reactor core). The plant shall be designed so that it can be brought into a controlled state and the containment function can be maintained, with the result that the possibility of plant states arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'.14 The effectiveness of provisions to ensure the functionality of the containment could be analysed on the basis of the best estimate approach.	
1	5.28	5.28. The design extension conditions shall be used to define the design basis for safety features and for the design of all other items important to safety that are necessary for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences.	5.28. The design extension conditions shall be used to define the design specifications for safety features and for the design of all other items important to safety that are necessary for preventing such conditions from arising, or, if they do arise, for controlling them and mitigating their consequences.	- minor change

Ref	Section	Old Requirements	Revised Requirement	Comment
1	5.31	5.31. The design shall be such that design extension conditions that could lead to significant radioactive releases are practically eliminated (see footnote 1). If not, for design extension conditions that cannot be practically eliminated, only protective measures that are of limited scope in terms of area and time shall be necessary for protection of the public, and sufficient time shall be made available to implement these measures.	5.31. The design shall be such that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'.16	- focus on preventing early or large radiation releases
1	5.31A		5.31A. The design shall be such that for design extension conditions, protective actions that are limited in terms of lengths of time and areas of application shall be sufficient for the protection of the public, and sufficient time shall be available to take such measures.	- ensure that protective actions take into account sufficient length of time
Requirement 32: Design for optimal operator performance				
1	5.55	5.55. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the effects of operating errors on safety. The design process shall pay attention to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant.	5.55. The design shall support operating personnel in the fulfilment of their responsibilities and in the performance of their tasks, and shall limit the likelihood and the effects of operating errors on safety. The design process shall give due consideration to plant layout and equipment layout, and to procedures, including procedures for maintenance and inspection, to facilitate interaction between the operating personnel and the plant, in all plant states.	- focus on both likelihood and effects of operating errors on safety

Ref	Section	Old Requirements	Revised Requirement	Comment
Requirement 33: Safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant				
1	Req 33	Safety systems shall not be shared between multiple units unless this contributes to enhanced safety.	Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.	- requirement for separate safety systems for each unit in a multiple unit plant
1	5.63	5.63. Safety system support features and safety related items shall be permitted to be shared between several units of a nuclear power plant if this contributes to safety. Such sharing shall not be permitted if it would increase either the likelihood or the consequences of an accident at any unit of the plant.	5.63. To further enhance safety, means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design.	- focus on interconnections between units in a multiple unit plant
Requirement 42: Safety analysis of the plant design				
1	5.73	5.73. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant.	5.73. The safety analysis shall provide assurance that uncertainties have been given adequate consideration in the design of the plant and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases.	- addition of "and in particular that adequate margins are available to avoid cliff edge effects and early radioactive releases or large radioactive releases."

Ref	Section	Old Requirements	Revised Requirement	Comment
1	5.75	5.75. The deterministic safety analysis shall mainly provide: (a) Establishment and confirmation of the design bases for all items important to safety; (b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant; (c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; (d) Comparison of the results of the analysis with dose limits and acceptable limits, and with design limits; (e) Demonstration that the management of anticipated operational occurrences and design basis accident conditions is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; (f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator.	5.75. The deterministic safety analysis shall mainly provide: (a) Establishment and confirmation of the design bases for all items important to safety; (b) Characterization of the postulated initiating events that are appropriate for the site and the design of the plant; (c) Analysis and evaluation of event sequences that result from postulated initiating events, to confirm the qualification requirements; (d) Comparison of the results of the analysis with acceptance criteria, design limits, dose limits and acceptable limits for purposes of radiation protection; (e) Demonstration that the management of anticipated operational occurrences and design basis accidents is possible by safety actions for the automatic actuation of safety systems in combination with prescribed actions by the operator; (f) Demonstration that the management of design extension conditions is possible by the automatic actuation of safety systems and the use of safety features in combination with expected actions by the operator.	- addition of comparison of results against "acceptable limits for purposes of radiation protection"

Ref	Section	Old Requirements	Revised Requirement	Comment
1	5.76	5.76. The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states, including shutdown, with particular reference to: (a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; (b) Providing assurance that small deviations in plant parameters that could give rise to large variations in plant conditions (cliff edge effects) will be prevented (see footnote 5); (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.	5.76. The design shall take due account of the probabilistic safety analysis of the plant for all modes of operation and for all plant states, including shutdown, with particular reference to: (a) Establishing that a balanced design has been achieved such that no particular feature or postulated initiating event makes a disproportionately large or significantly uncertain contribution to the overall risks, and that, to the extent practicable, the levels of defence in depth are independent; (b) Providing assurance that situations in which small deviations in plant parameters could give rise to large variations in plant conditions (cliff edge effects) will be prevented;20 (c) Comparing the results of the analysis with the acceptance criteria for risk where these have been specified.	- minor wording change re "cliff edge effects"
Requirement 53: Heat transfer to an ultimate heat sink				
1	Req 53	Systems shall be provided to transfer residual heat from items important to safety at the nuclear power plant to an ultimate heat sink. This function shall be carried out with very high levels of reliability for all plant states.	The capability to transfer heat to an ultimate heat sink shall be ensured for all plant states.	- simplified wording

Ref	Section	Old Requirements	Revised Requirement	Comment
1	6.19A		6.19A. Systems for transferring heat shall have adequate reliability for the plant states in which they have to fulfil the heat transfer function. This may require the use of a different ultimate heat sink or different access to the ultimate heat sink.	- focus on heat sinks
1	6.19B		6.19B. The heat transfer function shall be fulfilled for levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.	- focus on heat sinks in severe accidents
Requirement 58: Control of containment conditions				
1	6.28A		6.28A. Design provision shall be made to prevent the loss of the structural integrity of the containment in all plant states. The use of this provision shall not lead to an early radioactive release or a large radioactive release.	- focus on structural integrity of containment
1	6.28B		6.28B. The design shall also include features to enable the safe use of non-permanent equipment22 for restoring the capability to remove heat from the containment.	- addition of consideration of mobile equipment

Ref	Section	Old Requirements	Revised Requirement	Comment
Requirement 65: Control room				
1	6.39	6.39. Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room against hazards such as high radiation levels resulting from accident conditions, release of radioactive material, fire, or explosive or toxic gases.	6.39. Appropriate measures shall be taken, including the provision of barriers between the control room at the nuclear power plant and the external environment, and adequate information shall be provided for the protection of occupants of the control room, for a protracted period of time, against hazards such as high radiation levels resulting from accident conditions, releases of radioactive material, fire, or explosive or toxic gases.	- added "for a protected period of time"
1	6.40A		6.40A. The design of the control room shall provide an adequate margin against levels of natural hazards more severe than those considered for design, derived from the hazard evaluation for the site.	- focus on severe accidents
Requirement 67: Emergency response facilities on the site				
1	Req 67	An on-site emergency control centre, separate from both the plant control room and the supplementary control room, shall be provided from which an emergency response can be directed at the nuclear power plant.	The nuclear power plant shall include the necessary emergency response facilities on the site. Their design shall be such that personnel will be able to perform expected tasks for managing an emergency under conditions generated by accidents and hazards.	- focus on facilities necessary to manage an emergency under conditions generated by accidents and hazards

Ref	Section	Old Requirements	Revised Requirement	Comment
1	6.42	6.42. Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided in the on-site emergency control centre. The on-site emergency control centre shall provide means of communication with the control room, the supplementary control room and other important locations at the plant, and with on-site and offsite emergency response organizations. Appropriate measures shall be taken to protect the occupants of the emergency control centre for a protracted time against hazards resulting from accident conditions. The emergency control centre shall include the necessary systems and services to permit extended periods of occupation and operation by emergency response personnel.	6.42. Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided to the relevant emergency response facilities23. Each facility shall be provided with means of communication with, as appropriate, the control room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations.	- focus on all facilities necessary to manage an emergency both on-site and off-site
Requirement 68: Design for withstanding the loss of off-site power				
1	Req 68	The emergency power supply at the nuclear power plant shall be capable of supplying the necessary power in anticipated operational occurrences and accident conditions, in the event of the loss of off-site power.	The design of the nuclear power plant shall include an emergency power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power. The design shall include an alternate power source to supply the necessary power in design extension conditions.	- extends requirements to cover power supply for design extension conditions

Ref	Section	Old Requirements	Revised Requirement	Comment
1	6.43	6.43. In the design basis for the emergency power supply at the nuclear power plant, due account shall be taken of the postulated initiating events and the associated safety functions to be performed, to determine the requirements for capability, availability, duration of the required power supply, capacity and continuity.	6.43. The design specifications for the emergency power supply and for the alternate power source at the nuclear power plant shall include the requirements for capability, availability, duration of the required power supply, capacity and continuity.	- removes constraint to only consider design basis events
1	6.44A		6.44A. The alternate power source shall be capable of supplying the necessary power to preserve the integrity of the reactor coolant system and to prevent significant damage to the core and to spent fuel in the event of the loss of off-site power combined with failure of the emergency power supply.	- addresses requirements to deal with station blackouts
1	6.44B		6.44B. Equipment that is necessary to mitigate the consequences of melting of the reactor core shall be capable of being supplied by any of the available power sources.	- more specific requirements for mitigation of consequences of core melting
1	6.44C		6.44C. The alternate power source shall be independent of and physically separated from the emergency power supply. The connection time of the alternate power source shall be consistent with the depletion time of the battery.	- requirements on alternate power source

Ref	Section	Old Requirements	Revised Requirement	Comment
1	6.44D		6.44D. Continuity of power for the monitoring of the key plant parameters and for the completion of short term actions necessary for safety shall be maintained in the event of loss of the AC (alternating current) power sources.	- focus on monitoring of key plant parameters
1	6.45A		6.45A. The design shall also include features to enable the safe use of non-permanent equipment to restore the necessary electrical power supply.	- focus on mobile equipment to restore electrical power
Requirement 80: Fuel handling and storage systems				
1	6.68	6.68. For reactors using a water pool system for fuel storage, the design of the plant shall include the following: (a) Means for controlling the temperature, water chemistry and activity of any water in which irradiated fuel is handled or stored; (b) Means for monitoring and controlling the water level in the fuel storage pool and means for detecting leakage; (c) Means for preventing the uncovering of fuel assemblies in the pool in the event of a pipe break (i.e. anti-siphon measures).	6.68. For reactors using a water pool system for fuel storage, the design shall be such as to prevent the uncovering of fuel assemblies in all plant states that are of relevance for the spent fuel pool so that the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release is 'practically eliminated'26 and so as to avoid high radiation fields on the site. The design of the plant: (a) Shall provide the necessary fuel cooling capabilities; (b) Shall provide features to prevent the uncovering of fuel assemblies in the event of a leak or a pipe break; (c) Shall provide a capability to restore the water inventory. The design shall also include features to enable the safe use of non-permanent equipment to ensure sufficient water inventory for the long term cooling of	- emphasis on cooling fuel storage system to make possibility of early radioactive release "practically eliminated"

Ref	Section	Old Requirements	Revised Requirement	Comment
			spent fuel and for providing shielding against radiation.27	
1	6.68A		6.68A. The design shall include the following: (a) Means for monitoring and controlling the water temperature for operational states and for accident conditions that are of relevance for the spent fuel pool; (b) Means for monitoring and controlling the water level for operational states and for accident conditions that are of relevance for the spent fuel pool; (c) Means for monitoring and controlling the activity in water and in air for operational states and means for monitoring the activity in water and in air for accident conditions that are of relevance for the spent fuel pool; (d) Means for monitoring and controlling the water chemistry for operational states.	- requirements for monitoring and control of water temperature in fuel storage pool
Requirement 8: Performance of safety related activities				
2	4.31	4.31. The responsibilities and authorities for restarting a reactor after an event leading to an unplanned shutdown, scram or major transient, or to an extended period of maintenance, shall be clearly established in writing. An investigation shall be carried out to determine the cause of the event and corrective actions shall be taken to make its recurrence less likely. Prior to the restart or the resumption of full power	4.31. The responsibilities and authorities for restarting a reactor after an event leading to an unplanned shutdown, scram or major transient, or to an extended period of maintenance, shall be clearly established in writing. An investigation shall be carried out to determine the cause of the event (by means of root cause analysis wherever necessary) and corrective actions shall be taken to make its recurrence less	- addition of root cause analysis wherever necessary

Ref	Section	Old Requirements	Revised Requirement	Comment
		of the affected plant, the operating organization shall carry out necessary remedial actions, including inspection, testing and repair of damaged structures, systems and components, and shall revalidate the safety functions that might be challenged by the event. Restart conditions and criteria shall be established and followed after the timely implementation of the necessary corrective actions.	likely. Prior to the restart or the resumption of full power of the affected plant, the operating organization shall carry out necessary remedial actions, including inspection, testing and repair of damaged structures, systems and components, and shall revalidate the safety functions that might be challenged by the event. Restart conditions and criteria shall be established and followed after the timely implementation of the necessary corrective actions	
Requirement 12: Periodic safety review				
2	4.44	4.44. Safety reviews shall be carried out at regular intervals. Safety reviews shall address, in an appropriate manner, the consequences of the cumulative effects of plant ageing and plant modification, equipment requalification, operating experience, current standards, technical developments, and organizational and management issues, as well as siting aspects. Safety reviews shall be aimed at ensuring a high level of safety throughout the operating lifetime of the plant.	4.44. Safety reviews such as periodic safety reviews or safety assessments under alternative arrangements shall be carried out throughout the lifetime of the plant, at regular intervals and as frequently as necessary (typically no less frequently than once in ten years). Safety reviews shall address, in an appropriate manner: the consequences of the cumulative effects of plant ageing and plant modification; equipment requalification; operating experience, including national and international operating experience; current national and international standards; technical developments; organizational and management issues; and site related aspects. Safety reviews shall be aimed at ensuring a high level of safety	- more specific requirements on the timing and scope of periodic safety reviews

Ref	Section	Old Requirements	Revised Requirement	Comment
			throughout the operating lifetime of the plant.	
2	4.47	4.47. On the basis of the results of the systematic safety assessment, the operating organization shall implement any necessary corrective actions and reasonably practicable modifications for compliance with applicable standards aiming at enhancing the safety of the plant	4.47. On the basis of the results of the systematic safety assessment, the operating organization shall implement any necessary corrective actions and reasonably practicable modifications for compliance with applicable standards with the aim of enhancing the safety of the plant by further reducing the likelihood and the potential consequences of accidents.	- focus on enhancing safety by reducing likelihood and potential consequences of accidents
Requirement 18: Emergency preparedness				
2	5.6	5.6. The emergency plan shall be tested in exercises before the commencement of fuel loading. Emergency preparedness exercises shall be planned and conducted at suitable intervals, to evaluate the preparedness of plant staff and staff from external response organizations to perform their tasks, and to evaluate their cooperation in coping with an emergency and in improving the efficiency of the response.	5.6. The emergency plan shall be tested and validated in exercises before the commencement of fuel loading. Emergency preparedness training, exercises and drills shall be planned and conducted at suitable intervals, to evaluate the preparedness of plant staff and staff from external response organizations to perform their tasks, and to evaluate their cooperation in coping with an emergency and in improving the efficiency of the response [1, 6].	- addition of validation of emergency plan

Ref	Section	Old Requirements	Revised Requirement	Comment
2	5.7	5.7. Facilities, instruments, tools, equipment, documentation and communication systems to be used in an emergency shall be kept available and shall be maintained in good operational condition in such a manner that they are unlikely to be affected by, or made unavailable by, accident conditions.	5.7. Facilities, instruments, tools, equipment, documentation and communication systems to be used in an emergency, including those needed for off-site communication and for the accident management programme, shall be kept available. They shall be maintained in good operational condition in such a manner that they are unlikely to be affected by, or made unavailable by, accidents. The operating organization shall ensure that relevant information on safety parameters is available in the emergency response facilities and locations, as appropriate, and that communication between the control rooms and these facilities and locations is effective in the event of an accident [2]. These capabilities shall be tested periodically	- more specific requirements on facilities for emergency management
Requirement 19: Accident management programme				
2	Req 19	The operating organization shall establish an accident management programme for the management of beyond design basis accidents.	The operating organization shall establish, and shall periodically review and as necessary revise, an accident management programme.	- addition of requirement for periodic review of accident management programme

Ref	Section	Old Requirements	Revised Requirement	Comment
2	5.8	5.8. An accident management programme shall be established that covers the preparatory measures and guidelines that are necessary for dealing with beyond design basis accidents. The accident management programme shall be documented and periodically reviewed and revised as necessary. It shall include instructions for utilization of the available equipment — safety related equipment as far as possible, but also conventional equipment — and the technical and administrative measures to mitigate the consequences of an accident. The accident management programme shall also include organizational arrangements for accident management, communication networks and training necessary for the implementation of the programme.	5.8. An accident management programme shall be established that covers the preparatory measures, procedures and guidelines, and equipment that are necessary for preventing the progression of accidents, including accidents more severe than design basis accidents, and for mitigating their consequences if they do occur. The accident management programme shall be documented and shall be periodically reviewed and as necessary revised.	- addition of coverage of design extension conditions by the accident management programme
2	5.8A		5.8A. For a multi-unit nuclear power plant site, concurrent accidents affecting all units shall be considered in the accident management programme. Trained and experienced personnel, equipment, supplies and external support shall be made available for coping with concurrent accidents. Potential interactions between units shall be considered in the accident management programme.	- requirements for accident management of multiple unit plants

Ref	Section	Old Requirements	Revised Requirement	Comment
2	5.8B		5.8B. The accident management programme shall include instructions for the utilization of available equipment — safety related equipment as far as possible, but also items not important to safety (e.g. conventional equipment).	- requirement to include items not important to safety in the scope of the accident management programme
2	5.8C		5.8C. The accident management programme shall include contingency measures, such as an alternative supply of cooling water and an alternative supply of electrical power, to mitigate the consequences of accidents, including any necessary equipment. This equipment shall be located and maintained so as to be functional and readily accessible when needed.	- requirement to consider alternate sources of cooling water and electrical power
2	5.8D		5.8D. The accident management programme shall include the technical and administrative measures necessary to mitigate the consequences of an accident.	- inclusion of technical and administrative measures
2	5.8E		5.8E. The accident management programme shall include training necessary for implementation of the programme.	- inclusion of training

Ref	Section	Old Requirements	Revised Requirement	Comment
2	5.8F		5.8F. In developing the accident management programme and its procedures, the possibility of regional infrastructure being degraded and of adverse working conditions (e.g. elevated radiation levels, elevated temperatures, lack of lighting, limited access to the plant from off the site) for operators, as well as the possibility of operating conditions for equipment being degraded, shall be taken into account so as to ensure that actions expected for accident management will be feasible and will be able to be taken in a timely and reliable manner.	- requirement to take into account degradation of regional infrastructure
2	5.9	5.9. Arrangements for accident management shall provide the operating staff with appropriate systems and technical support in relation to beyond design basis accidents. These arrangements and guidance shall be available before the commencement of fuel loading and they shall address the actions necessary following beyond design basis accidents, including severe accidents. In addition, arrangements shall be made, as part of the emergency plan, to expand the emergency response arrangements, where necessary, to include the responsibility for long term actions.	5.9. Arrangements for accident management shall provide the operating staff with appropriate competence, systems and technical support. These arrangements and relevant guidance shall be available before the commencement of fuel loading, shall be validated and shall then be periodically tested as far as practicable in exercises and used in training and drills [1, 6]. In addition, arrangements shall be made, as part of the accident management programme and the emergency plan, to expand the emergency arrangements, where necessary, to include the responsibility for long term actions.	- inclusion of requirements for training and drills

Ref	Section	Old Requirements	Revised Requirement	Comment
Requirement 22: Fire safety				
2	5.24	5.24. The operating organization shall be responsible for ensuring that appropriate procedures are in place for effectively coordinating and cooperating with all firefighting services involved. Periodic joint fire drills and exercises shall be conducted to assess the effectiveness of the fire response capability.	5.24. The operating organization shall be responsible for ensuring that appropriate procedures, equipment and staff are in place for effectively coordinating and cooperating with all firefighting services involved. Periodic joint fire drills and exercises shall be conducted to assess the effectiveness of the fire response capability.	- extending requirements to include appropriate equipment and staff
Requirement 24: Feedback of operating experience				
2	5.27	5.27. The operating organization shall establish and implement a programme to report, collect, screen, analyse, trend, document and communicate operating experience at the plant in a systematic way. It shall obtain and evaluate information on relevant operating experience at other nuclear installations to draw lessons for its own operations. It shall also encourage the exchange of experience within national and international systems for the feedback of operating experience. Relevant lessons from other industries shall also be taken into consideration, as necessary.	5.27. The operating organization shall establish and implement a programme to report, collect, screen, analyse, trend, document and communicate operating experience at the plant in a systematic way. It shall obtain and evaluate available information on relevant operating experience at other nuclear installations to draw and incorporate lessons for its own operations, including its emergency arrangements. It shall also encourage the exchange of experience within national and international systems for the feedback of operating experience. Relevant lessons from other industries shall also be taken into consideration, as necessary.	- minor wording change

Ref	Section	Old Requirements	Revised Requirement	Comment
2	5.32	5.32. The operating organization shall maintain liaison, as appropriate, with support organizations (manufacturers, research organizations and designers) involved in the design, in order to feed back information on operating experience and to obtain advice, if necessary, in the event of equipment failure or in other events.	5.32. The operating organization shall maintain liaison, as appropriate, with support organizations (e.g. manufacturers, research organizations and designers) involved in the design, construction, commissioning and operation of the plant in order to feed back information on operating experience and to obtain advice, if necessary, in the event of equipment failure or in other events.	- include construction and commissioning organizations in the scope of organizations from which feedback is sought
Requirement 26: Operating procedures				
2	7.3	7.3. Procedures shall be developed for use in the event of anticipated operational occurrences and design basis accidents. Emergency operating procedures and guidance for managing beyond design basis accidents shall also be developed. Both event based approaches and symptom based approaches shall be used, as appropriate. The related analysis and justifications shall be documented.	7.3. Procedures shall be developed and validated for use in the event of anticipated operational occurrences and design basis accidents. Guidelines or procedures shall be developed for the management of accidents more severe than the design basis accidents. Both event based approaches and symptom based approaches shall be used, as appropriate. The related analysis and justifications shall be documented.	- guidelines or procedures for management of accidents more severe than the design basis accidents added

Ref	Section	Old Requirements	Revised Requirement	Comment
Requirement 28: Material conditions and housekeeping				
2	7.10	7.10. Administrative controls shall be established to ensure that operational premises and equipment are maintained, well lit and accessible, and that temporary storage is controlled and limited. Equipment that is degraded (owing to leaks, corrosion spots, loose parts or damaged thermal insulation, for example) shall be identified, reported and corrected in a timely manner.	7.10. Administrative controls shall be established to ensure that operational premises and equipment are maintained, well lit and accessible, and that temporary storage is controlled and limited. Equipment that is degraded (owing to leaks, corrosion spots, loose parts or damaged thermal insulation, for example) shall be identified and reported and deficiencies shall be corrected in a timely manner.	- deficiencies corrected in a timely manner
Requirement 31: Maintenance, testing, surveillance and inspection programmes				
2	8.14A		8.14A. The operating organization shall establish maintenance programmes for non-permanent equipment to be used for accidents more severe than design basis accidents [2], in order to maintain high reliability of this equipment. The operating organization shall carry out periodic training and exercises in handling the equipment and connecting it to the nuclear power plant.	- include mobile equipment and training on the mobile equipment

APPENDIX 6 - Design Features to Deal with Causes of Unsafe Control Actions

This appendix documents the results of the step in the STPA analysis in Chapter 11 where design features that deal with the identified causes of unsafe control actions are identified. The results are shown for the following analyses:

- Utility Level – Technology Architecture
- Utility Level – Business Process Architecture
- Steam Generator Level Control
- Periodic Safety Review Process

For each of these analyses, there is a table that lists for each unsafe control action:

Potential Causes of the Unsafe Control Action (UCA): these causes are identified in Chapter 11

Design Feature from IAEA Principles: these were derived by examining the design principles in Appendix 3 and identifying which design features would address the potential causes of the UCA (along with the **Req#** indicating which requirement from Appendix 3 is being referenced)

Other Design Features: these were derived by examining the design features from the IAEA principles and then, based on design experience, identifying other features that would typically be used to address the potential cause of the UCA.

Utility Level – Technology Architecture **UCA: Not Providing Lower Power when required**				
No.	**Potential Cause of UCA**	**Req#**	**Design Feature from IAEA Principles**	**Other Design Features**
1	- incorrect setpoint provided to operator	23	Assumptions on operations and maintenance performance necessary to achieve safety are clearly documented	- robust design process - robust V&V - Effective OPEX and Timely Change Control
2	- operator did not correctly understand the required setpoint to be set	78	Establish a program to ensure personnel assigned to safety related activities have the necessary competencies to perform the activities assigned to them Establish a staffing plan that ensures that sufficient competent staff are available to perform safety related activities Establish policies for scheduling of personnel for safety related activities to ensure that sufficient time is allocated to adequately perform the activities Establish a staff health policy that ensures staff are fit for duty	- 3 way communications - clear documentation of the setpoint - trained and competent operators
		23	Operations and maintenance personnel are involved in effective design reviews to ensure that assumptions on operations and maintenance performance are achievable	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
3	- changes to the setpoint not communicated to operator in a timely manner	85	Establishment of a risk management program that ensures that risks are identified, analyzed and reduced to levels as low as reasonably achievable. All activities important to safety shall be carried out in accordance with written procedures to ensure that the plant is operated within the established operational limits and conditions. Written communication shall be preferred and spoken communication shall be minimized. If spoken communication is used, attention shall be given to ensuring that spoken instructions are clearly understood. Aspects of the working environment that influence human performance factors (such as workload or fatigue) and the effectiveness and fitness of personnel for duty shall be identified and controlled. The operating organization shall encourage plant personnel to have a questioning attitude and to make appropriate and conservative decisions, so as to minimize risk and to maintain the plant in a safe condition.	- Effective change control process - prioritization of work based on safety impacts - Impact assessment of all proposed changes from a safety perspective to identify the need for a change to the setpoint

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
4	- error in specifying trip algorithm	19	The design of items important to safety shall take into account the attributes of manufacturability, constructability and installability to ensure that the probability of introduction of undetected errors is commensurate with the level of risk of errors. Operating experience from the design, construction and operation of similar plants shall be taken into account.	- Clear interface between process designer and I&C designer - effective V&V - Effective design process - Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner
		28	Technical specifications for items important to safety shall be developed using appropriate methods that result in complete and correct specifications of safety requirements. Procured items important to safety shall be qualified as being compliant with safety requirements The qualification of procured items shall include a hazard analysis to determine if there are any new hazards introduced by the use of the item	
		152	Conservative design, construction and testing practices commensurate with safety objectives Compliance with appropriate codes and standards Proven methods of manufacturing and construction	
		153	Quality assurance applied to ensure with high level of confidence that safety requirements and objectives are met	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
5	- error in implementation of trip logic		- see 4	- Clear interface between process designer and I&C designer - effective V&V - Effective design process - Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner
6	- inadequate V&V to detect error in trip logic		- see 4	- Effective V&V

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
7	- changes to control logic not implemented in a timely manner	61	Establish and implement a program for the planning and execution of online and offline maintenance and design modification activities	- Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner
		69	Establishment of a program for identification and effective communication with parties interested in the safety of the plant	
		71	Establishment of a safety management system that takes into account the safety significance of changes	
		81	Establish a safety management system that ensuring the continuing safety of the plant design. Designate an individual to be responsible for the safety of the plant design	
		84	Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner. Establish a program to investigate events with significant implications for safety and take effective actions to avoid reoccurrence of the events.	
		88	Establishment of a set of programs necessary to achieve and maintain safety along with the establishment of an effective management system for the programs	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
8	- error in specification of process model		- see 4	- Clear interface between process designer and I&C designer - effective V&V - Effective design process - Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner
9	- error in implementation of process model logic		- see 4	- Clear interface between process designer and I&C designer - effective V&V - Effective design process - Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner
10	- changes to process model logic not implemented in a timely manner		- see 7	- Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
11	- time lags and inaccuracies not accounted for in the specification of the process model		see 4	- Clear interface between process designer and I&C designer - effective V&V - Effective design process - Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner
12	- communication of setpoint or setpoint changes to operator not done		see 2	- 3 way communications - clear documentation of the setpoint
13	- communication of setpoint was unclear		- see 2	- 3 way communications - clear documentation of the setpoint
14	- delays in setting new setpoint		- see 4	- prioritization of work takes into account safety significance of work

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
15	- loss of power in automated controller HMI	150	Principal emphasis is placed on the primary means of achieving safety, which is the prevention of accidents Hazards shall be eliminated if possible Remaining hazards shall be controlled to make their probability of occurrence as low as reasonably achievable	- Reliable sources of power - Redundant sources of power - diverse sources of power
		169	Automatic systems are provided that would safely shut down the reactor, maintain it in a shut down and cooled state, and limit any release of fission products that might possibly ensue, if operating conditions were to exceed predetermined set points.	
		170	Reliability targets are assigned to safety systems or functions. The targets are established on the basis of the safety objectives and are consistent with the roles of the systems or functions in different accident sequences. Provision is made for testing and inspection of components and systems for which reliability targets have been set.	
		188	Nuclear plants are so designed that the simultaneous loss of on-site and off-site AC electrical power (a station blackout) will not soon lead to fuel damage.	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
16	- error in automated controller HMI		- see 4	- Clear interface between process designer and I&C designer - effective V&V - Effective design process - Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner
17	- delayed transmission of control action by HMI		- see 4	- qualified components - graded QA requirements commensurate with safety significance - effective preventive maintenance program - effective ageing management program

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
18	- component failures	172	Safety components and systems are chosen that are qualified for the environmental conditions that would prevail if they were required to function. The effects of ageing on normal and abnormal functioning are considered in design and qualification.	- qualified components - graded QA requirements commensurate with safety significance - effective preventive maintenance program - effective ageing management program
		206	Safety related structures, system and components are subject to regular maintenance, inspection and testing as necessary to ensure that they perform consistent with safety requirements over the life of the plant	
		40	• Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements • Design margins established to account for unanticipated failures. • Robust technical justification for the inspection and maintenance program.	
		44	Establish an ageing management program to maintain the performance of structures, systems and components that have an impact on safety	
		60	Establish a maintenance program for all equipment that is related to performing safety functions in the plant	
		152	• Conservative design, construction and testing practices commensurate with safety objectives • Compliance with appropriate codes and standards • Proven methods of manufacturing and construction •	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
19	- incorrect gain	201	Normal plant operations are controlled by detailed, validated and formally approved procedures	- Effective maintenance program - Effective ageing management program
		40	Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements Design margins established to account for unanticipated failures. Robust technical justification for the inspection and maintenance program.	
		55	Establish and implement a commissioning program that demonstrates that the plant as built is compliant with all design assumptions and licensing conditions Establish operating and maintenance procedures necessary to keep the plant operating within its safe operating envelope and validate the procedures as part of the commissioning program	
20	- incorrect compensation of flux detector signal		- see 19	- Effective maintenance program - Effective ageing management program
21	- failures in sensors, communication lines or power		- see 18	- Qualified components - Effective maintenance program - Effective ageing management program

Utility Level – Business Process Architecture **UCA: Utility Non-compliant and Changes not made in a Timely Manner**				
No.	**Potential Cause of UCA**	**Req#**	**Design Feature from IAEA Principles**	**Other Design Features**
1	- change implemented poorly	72	Establishment of a safety management system that is clearly documented Establishment of a document and records management system so that all safety related documents are controlled and the correct version of documents and records are available to personnel requiring them	Adequate verification and validation of implementations to provide confidence that change has been implemented consistent with safety and quality requirements
2	- scope of change inconsistent with current state of utility	30	Documented safety management plan Compliance of safety management plan with industry standards Understanding of all personnel on their role in the safety management plan Assessments and audits of compliance with safety management plan	- sufficient assessments of compliance of processes with documented expectations
3	- implementation of change results in hazard not previously present	81	Establish a safety management system that ensuring the continuing safety of the plant design. Designate an individual to be responsible for the safety of the plant design	Adequate verification and validation of implementations to provide confidence that change has been implemented consistent with safety and quality requirements

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
4	- assessment reports not produced in a timely manner	82	Establish periodic safety reviews of the plant, processes, organizations and governance Establish continuous improvement process taking input from periodic safety review and operational experience both internal and external to the organization	Adequate management oversight of assessments
5	- assessors not qualified	156	Personnel involved with safety related activities have the competencies necessary to perform their duties Possibility of human error is taken into account	Management oversight to ensure that personnel have required qualifications
6	- assessment based on inaccurate information"	157	Safety assessment done before construction and operation begins Safety assessment is performed independently and documented in a third party reviewable manner	Adequate configuration management

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
7	- documentation of current state not up'-to'-date	160	Operational excellence is achieved by: augmenting safety culture and defence in depth; improving human performance; maintaining excellent material condition and equipment performance; using self-assessments and peer reviews; exchanging operating experience and other information around the world; increasing application of PSAs; and extending the implementation of severe accident management.	Adequate configuration management

Steam Generator Level Control **UCA: Not Increasing Flow When Level is Less than Setpoint – Margin**				
No.	**Potential Cause of UCA**	**Req#**	**Design Feature from IAEA Principles**	**Other Design Features**
1	incorrect setpoint set	179	Components, structures, and systems used during startup, low power and shutdown operations are designed to maintain or restore the reactivity control, decay heat removal, and the integrity of the fission product barriers, so as to prevent the release of radioactive material resulting from accidents initiated during those operations.	- robust design process - robust V&V - Effective OPEX and Timely Change Control
		198	Operation and maintenance staff are trained and qualified to perform their duties in accordance with approved procedures	
		199	Training programs in place to ensure that personnel responsible for safety related tasks have the necessary competencies	
		210	Equipment, instrumentation and diagnostic aids are available to operators, who may at some time be faced with the need to control the course and consequences of an accident beyond the design basis.	
2	incorrect margin set		See 1 above	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
3	required changes to setpoint or margin not made in a timely manner	18	controlling changes to the design to ensure assurance that safety requirements are satisfied is maintained at the same level or better when changes are made to the design	- Effective change control process - prioritization of work based on safety impacts - Impact assessment of all proposed changes from a safety perspective to identify the need for a change to the setpoint
		42	Establishment of controls on plant configuration that ensures changes to plant configuration are consistent with the established safe operating envelope	
		43	Establishment of a design modification process that is compliant with relevant national and international standards, and is based on proven engineering practices Design modification process includes proper design and safety reviews, implementation and testing Establishment of controls over the configuration of the physical plant and its design including a limit on the number of temporary modifications and limits on the time they may be in effect	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
4	control algorithm not specified correctly	152	Conservative design, construction and testing practices commensurate with safety objectives Compliance with appropriate codes and standards Proven methods of manufacturing and construction	- Clear interface between process designer and I&C designer - effective V&V - Effective design process - Effective use of OPEX to identify needed changes - Effective change control process to implement changes in a timely manner
		153	Quality assurance applied to ensure with high level of confidence that safety requirements and objectives are met	
		191	Clear, complete and correct specifications for safety related equipment	
		28	Technical specifications for items important to safety shall be developed using appropriate methods that result in complete and correct specifications of safety requirements. Procured items important to safety shall be qualified as being compliant with safety requirements The qualification of procured items shall include a hazard analysis to determine if there are any new hazards introduced by the use of the item	
5	control algorithm not implemented correctly		See 4 above	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
6	automated controller not able to meet performance requirements	40	Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements Design margins established to account for unanticipated failures. Robust technical justification for the inspection and maintenance program.	
		83	Effective equipment qualification programs to provide confidence that equipment will satisfy its safety requirements	
7	required changes to control algorithm not implemented in a timely manner		See 3 above	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
8	failure of automated controller	4	Design utilizes defense-in-depth principle to achieve control, cool and contain with a high degree of confidence.	- Reliable sources of power - Redundant sources of power - diverse sources of power
		14	The design takes into account interactions between systems to ensure that failures of systems providing redundant or diverse safety functionality do not have common cause failures.	- qualified components - graded QA requirements commensurate with safety significance - effective preventive maintenance program - effective ageing management program
		40	Inspection and preventive maintenance programs established to maintain equipment performance consistent with safety requirements Design margins established to account for unanticipated failures. Robust technical justification for the inspection and maintenance program.	
		60	Establish a maintenance program for all equipment that is related to performing safety functions in the plant	
9	loss of power to automated controller		See 8 above	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
10	mismatch between state of model and actual level in steam generator		See 14 through 17 below	
11	error in implementation of feedwater control valve		See 8 above	
12	failure of feedwater control valve		See 8 above	
13	loss of power to feedwater control valve		See 8 above	
14	error in implementation of level sensor		See 8 above	
15	failure of level sensor		See 8 above	
16	loss of power to level sensor		See 8 above	
17	level sensor is inaccurate		See 8 above	

Periodic Safety Review Process **UCA: Perform Periodic Safety Review – no findings when opportunities available**				
No.	**Potential Cause of UCA**	**Req#**	**Design Feature from IAEA Principles**	**Other Design Features**
1	standards, requirements, plant design basis documents and/or any information required for review of a safety factor area either does not exist, is not current, is missing or is incorrect.	38	Establishment of clear expectations on the documentation, revisions control and communication of the safety management system	- comprehensive set of standards and requirements established necessary to comply with all regulatory requirements
		41	Establishment of controls over the configuration of the physical plant and its design	-comprehensive set of design basis documentation
		75	A complete set of operating limits and conditions are documented and consistent with design assumptions and intent	- comprehensive set of plant design documentation for all safety related structures, systems and components
		84	Establish a program to collect, analyze and communicate operating experience at the plant in a systematic manner.	- comprehensive set of operating history documentation
		159	Operating experience and research relevant to safety is used to identify areas for improvement to safety	
2	standards and/or requirements do not match the safety factor area as implemented"			

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
3	no definition of the business process to conduct periodic safety reviews	34	Expectation that safety goals are periodically reviewed against organizational strategies and plans are established	- clear expectations on the need for a periodic safety review
		36	Expectations that the safety management system be developed, applied and continuously improved shall be established	- clear procedures for the conduct of periodic safety reviews
		74	Safety policies establishing the priority for safety and the standards to be met for all safety related activities	
		81	Establish a safety management system that ensuring the continuing safety of the plant design	
		86	Establish an audit and review program to ensure that the safety management program has been effectively implemented and continuously improved over time	
		88	Establishment of a set of programs necessary to achieve and maintain safety along with the establishment of an effective management system for the programs	
		94	Expectation that safety goals are periodically reviewed against organizational strategies and plans are established	
		154	Self-assessment used to evaluate effectiveness of processes against pre-established expectations	
		155	Peer review used to identify areas for improvement	
		197	Ongoing, independent safety reviews in place	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
4	decision makers not adequately trained in requirements for performing periodic safety reviews	41	Establishment of governance that focuses on optimizing safety by keeping radiation risks as low as reasonably achievable	- definition of qualifications for decision makers for periodic safety review initiation includes requirements on periodic safety reviews
		41	Establishment of a program to establish the necessary competencies required within the operating organization and the development and training program to maintain the required competencies	- training established and delivered to decision makers for periodic safety review initiation
		43	Establishment of a program to establish the necessary competencies required within the operating organization and the development and training program to maintain the required competencies	
		74	Programs to communicate and train personnel in the safety policies	
		75	A training program is established to ensure that personnel assigned safety related activities are knowledgeable of the operating limits and conditions	
		65	Programs to educate personnel their role in achieving and maintaining safety	
		79	Clear definitions for the qualifications and competencies of personnel assigned to safety related activities are documented.	
		79	Governance for assigning personnel to safety related tasks includes confirmation that the personnel have the necessary qualifications and competencies	
		79	Establishment of a training program that ensures that personnel assigned to safety related tasks have the necessary qualifications and competencies	
		156	Personnel involved with safety related activities have the competencies necessary to perform their duties	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
5	inadequate budget allocated to support PSR	36	The safety management system shall be integrated into the overall management system	- need for periodic safety reviews is included in business planning process
6	inadequate staffing of personnel with the required skills for PSR			- business planning includes identification of staff levels of qualified staff able to conduct PSR activities in all required areas
7	responsibility for initiating a PSR not defined	41	Clear responsibility for the safety of the plant within the operating organization's management system	- clear responsibility is established for the initiation of periodic safety reviews
		81	Designate an individual to be responsible for the safety of the plant design	
		147	During the operation and maintenance phase, the operating organization has the overriding responsibility for safety	
		147	Responsibility for safety is in no way diluted by activities and responsibilities of designers, suppliers, constructors or regulators	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
8	inadequate understanding by decision makers on the scope and personnel requirements necessary to conduct an effective PSR	74	Continuous improvement program focused on operational safety	- definition of qualifications for decision makers for periodic safety review initiation includes requirements on periodic safety reviews
		75	A continuous improvement program is established that revises operating limits and conditions based on operating experience	- training established and delivered to decision makers for periodic safety review initiation
9	inadequate priority given to conducting the PSR	65	Clearly defined responsibilities for all managers to advocate and support a safety culture	- decision makers for initiating periodic safety reviews demonstrate a safety culture by prioritizing PSR scheduling appropriately
		65	Safety policies establishing the priority for safety and the standards to be met for all safety related activities	
		74	Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety	
10	perception that the current state of all safety factors is acceptable and hence scheduling a PSR is a low priority			- decision makers for initiating periodic safety reviews demonstrate a safety culture by prioritizing PSR scheduling appropriately

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
11	lack of understanding on the frequency for conducting a PSR			- definition of qualifications for decision makers for periodic safety review initiation includes requirements on periodic safety reviews
12	priority and/or expectations for the performance of PSR not clearly communicated	65	Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety	- decision makers for initiating periodic safety reviews demonstrate a safety culture by prioritizing PSR scheduling appropriately
		74	Clear leadership role for senior managers to demonstrate and communicate the utmost priority of safety	- clear documentation of need for PSR and its priority is established as part of business planning
		85	Written communication shall be preferred and spoken communication shall be minimized. If spoken communication is used, attention shall be given to ensuring that spoken instructions are clearly understood.	
13	responsibilities for performing PSR in each safety factor area is not clearly defined and/or communicated	86	Establish the organization responsible for audit and review to have sufficient authority and organizational independence to be able to identify problems, to recommend solutions and to verify that solutions have been effectively implemented.	- decision maker for initiating PSR clearly communicates to each organization assigned responsibility for a portion of the PSR
14	lack of establishing effective performance measures that reflect the current state of each safety factor area			- performance measures are defined and measured for all safety factor areas supporting the PSR

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
15	need to conduct PSR is not communicated in a timely manner to allow the needs to be incorporated into business plans			- business planning includes identification of staff levels of qualified staff able to conduct PSR activities in all required areas
16	hiring of staff with the appropriate knowledge and skills results in delays to performance of the PSR			- business planning includes identification of staff levels of qualified staff able to conduct PSR activities in all required areas
17	human error	85	Written communication shall be preferred and spoken communication shall be minimized. If spoken communication is used, attention shall be given to ensuring that spoken instructions are clearly understood.	- the possibility of human error is taken into account with appropriate checks and balances for all PSR tasks

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
18	organizations and personnel assigned to perform the PSR do not have the necessary skills and knowledge	41	Establishment of governance that focuses on optimizing safety by keeping radiation risks as low as reasonably achievable	- definition of qualifications for decision makers for periodic safety review initiation includes requirements on periodic safety reviews
		41	Establishment of a program to establish the necessary competencies required within the operating organization and the development and training program to maintain the required competencies	- training established and delivered to decision makers for periodic safety review initiation
		43	Establishment of a program to establish the necessary competencies required within the operating organization and the development and training program to maintain the required competencies	
		74	Programs to communicate and train personnel in the safety policies	
		75	A training program is established to ensure that personnel assigned safety related activities are knowledgeable of the operating limits and conditions	
		65	Programs to educate personnel in their role in achieving and maintaining safety	
		79	Clear definitions for the qualifications and competencies of personnel assigned to safety related activities are documented.	
		79	Governance for assigning personnel to safety related tasks includes confirmation that the personnel have the necessary qualifications and competencies	
		79	Establishment of a training program that ensures that personnel assigned to safety related tasks have the necessary qualifications and competencies	
		156	Personnel involved with safety related activities have the competencies necessary to perform their duties	

No.	Potential Cause of UCA	Req#	Design Feature from IAEA Principles	Other Design Features
19	PSR findings and recommendations not communicated to requesters in a timely manner	85	Written communication shall be preferred and spoken communication shall be minimized. If spoken communication is used, attention shall be given to ensuring that spoken instructions are clearly understood.	- expectations established for the documentation of all PSR findings and recommendations and the schedule for their production and communication