Modeling and Assessment of Emergency Mitigation Preparedness & Vulnerability for External Events in Nuclear Power Plants

Modeling and Assessment of Emergency Mitigation Preparedness & Vulnerability for External Events in Nuclear Power Plants

by

AHMAD ASSI

Mech. Eng (Honors)

A Thesis

Submitted to the School of Graduate Studies

in Partial Fulfillment of the Requirements for the Degree

Master of Applied Science in Engineering Physics

McMaster University

MASTER OF APPLIED SCIENCE (2014)
(Engineering Physics)

MCMASTER UNIVERSITY
Hamilton, Ontario, Canada

Title: Modeling and Assessment of Emergency Mitigation Preparedness & Vulnerability for External Events in Nuclear Power Plants

Author: Ahmad Assi
Mechanical Engineering (Honors)
Ryerson University

Supervisor: Dr. J. C. Luxat
Department of Engineering Physics
McMaster University

Number of Pages: xviii / 128

Acknowledgments

I would like to express my gratitude to everyone who supported me throughout the course of my program study and through the writing of this thesis. I am thankful for their aspiring guidance and advice. I am sincerely grateful to them for sharing their knowledge and experience on a number of issues related to this thesis.

My sincere thanks to my supervising professor Dr. John Luxat for sharing his valuable expertise in the industry, his steady support and guidance in writing this thesis paper.

I would also like to thank my parents, my wife, my two beautiful boys and family for their support, encouragement and giving me the drive and reasons to persevere and succeed in my work and studies.

To My

Beautiful Family

Thesis Abstract

Current Nuclear Power Plant (NPP) design does not account for Beyond Design Basis Events (BDBEs) and thus lack the provisions to effectively mitigates complete loss of AC power and total loss of heat sink. Furthermore, parametric models used in PRA studies to assess Nuclear Power Plant's safety risk for BDBE and External Events (EE) have significant limitations and proved ineffective to provide solutions on how to mitigate in BDBE or EEs situations. The Fukushima accident is a good example where PRA assessments did not provide the necessary means to cool or contain the reactors effectively. In this thesis, Emergency Mitigation Preparedness (*EMP*) model and assessment is proposed. The *EMP* model is objective and practical in evaluating NPP's mitigation readiness in BDBE and EEs situations and provide a practical *NPP Vulnerability* indicator gauge which can potentially be used in risk-informed decisions. This will aid further in the NPP to improve in areas of emergency planning, enhance site and reactor design and improve workers safety and readiness to execute effective mitigation procedures and emergency plans.

Executive Summary

This thesis discusses the evaluation of Nuclear Power Plants' (NPP) mitigation readiness and assesses NPPs vulnerability pertaining to severe accidents that may develop as a consequence of Beyond Design Basis Events (BDBEs). A particular emphasis is placed upon BDBEs initiated by extreme external events such as a External Flooding (including Tsunami events), External Fire, Severe Cold/Ice Storms, Extreme Wind events and Seismic. The thesis is divided into seven chapters as follow:

Chapter one will presents the progression of severe accidents in NPP due to BDBE and why the need for a better emergency mitigation preparedness is required. The thesis problem statement is also presented. Chapter two introduces current *IAEA safety standards in nuclear power plants* that deal with external hazards and analyzes the means to protect NPPs from such external hazards and concludes with a safety recommendation summary for external hazards. Chapter three discusses the *Common Cause Failure models* currently used in Probabilistic Risk Assessments (PRA) studies to evaluate the hazards faced by NPPs. The chapter introduces major models by providing models' description as well as illustrates models' limitations. Chapter four illustrates *mitigation consequences of severe accidents in NPP*. The chapter discusses various critical systems in an NPP (such as containment integrity, Hydrogen generation, loss of coolant, spent fuel and much more) and their potential impact on the NPP functionality and safety.

Chapter five introduces an assessment of the *Emergency Mitigation Preparedness* (*EMP*) model in NPP. The model is based on evaluating four factors (1) emergency equipment (2) NPP inherent safety features (3) Human factor and (4) NPP physical barriers. Also, external hazard relative risk ranking is introduced and incorporated into the *EMP* model. The model is explained in details via a discussion, flow charts and a logic diagrams. In chapter six, the *EMP* model is demonstrated by taking the March 11, 2011 Fukushima accident in Japan as a case study. The first case study evaluates the *EMP* and NPP Vulnerability using one external hazard - Tsunami. A second case study evaluates the EMP and NPP Vulnerability in multiple external hazard situations. Chapter seven provides discussion, conclusion and suggested future works.

This Page is left

Intentionally Blank

Table of Contents

List of Tables

List of Figures

List of Acronyms

Acronym	Definition
AC	Alternating Current
AF	Alpha Factor
AFW	Auxiliary Feed Water
Alpha-1	Emergency Equipment factor
Alpha-2	NPP Inherent Safety features
Alpha-3	Human Factor
Alpha-4	NPP Physical Barriers
AOP	Abnormal Operating Procedure
BDBE	Beyond Design Basis Event
BDEE	Beyond Design External Event
BF	Beta Factor
BFR	Binomial Failure Rate
BWR	Boiling Water Reactor
CANDU	Canada Deuterium Uranium Reactor
CCCG	Common Cause Component Group
CCF	Common Cause Failure
CFR	Code of Federal Regulation
CNSC	Canadian Nuclear Safety Commission
DC	Direct Current
ECFV	Emergency Containment Filtered Ventilation
EDG	Emergency Diesel Generator
EE	External Event
EMP	Emergency Mitigation Preparedness Model
EOP	Emergency Operating Procedure
FTA	Fault Tree Analysis

HPCI	High Pressure Coolant Injection
I & C	Instrumentation & Control
IAEA	International Atomic Energy Agency
LER	Licensee Event Report
Lethal Shock	A shock in which all components in a system are failed with certainty any time the shock occurs
Non-Lethal Shock	A shock that has some independent chance that each component it the system fails as a result of the shock
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
MGL	Multiple Greek Letter
NPP	Nuclear Power Plant
NPP Vulnerability	Relative likelihood to protect or to prevent undesirable consequence from occurring at NPP
NRC	U.S. Nuclear Regulatory Commission
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
SAMG	Severe Accident Management Guideline
SBO	Station Black-Out
SG	Steam Generator
Shock	A component failure state other than intrinsic, random or independent
SSC	System, Structure & Components
UHS	Ultimate Heat Sink
UPM	Unified Partial Method

This Page is left

Intentionally Blank

Chapter 1

Emergency Preparedness

1.1 Introduction

The nuclear industry accepted Chernobyl and Three Mile Island accidents as accidents attributed to operational and human errors. The industry responded by creating organizations such as WANO and INPO to prevent such accidents from occurring again by increasing shared operation experience and knowledge between nuclear operators. And then the Fukushima accident occurred on March 11, 2011 where a major earthquake struck the east cost of Japan, causing widespread damage due to a consequential massive Tsunami which was the primary cause for the worst nuclear disaster in nuclear generation history. The Fukushima nuclear power plant (NPP) failed to maintain safety functions to cool and contain the reactor core following the Beyond Design Basis Event (BDBE). The Tsunami resulted in a total loss of AC power across four units at the Fukushima Daiichi Nuclear Power station and a significant loss of safety equipment at the station. Due to complete station black-out (SBO) total heat sink was lost which led to severe core damage and off-site release of radioactive materials.

The Fukushima accident has sparked the nuclear agencies and NPP operators worldwide once again to review the adequacy of their plants to successfully manage events such as those which occurred at Fukushima. The World Association of Nuclear Operators (WANO) issued numerous Significant Operating Experience Reports - SOERs [22] (such as 2011-2/3/4 and 2013-2) to ensure NPPs emergency readiness to external events and mitigation readiness to name a few.

The Canadian regulator (CNSC) has issued specific Fukushima Action Items (FAIs) [23] for the CANDU fleet to upgrade their response capabilities to severe accidents due to Beyond Design Basis Events (BDBEs) such as external events.

1.2 Severe Accident Scenario

Severe accidents would typically be divided into two categories:

- Failure to shutdown the reactor core (loss of Shut Down System 1 and 2).
- Total loss of heat sink (this could be caused by loss of all cooling water or loss of all electrical power).

The aftermath of a BDBE is a potential extended loss of all AC power and consequentially the loss of total heat sink for the reactor core. The nuclear industry approach to mitigates this potential severe accidents (SA) can be summarized as follows:

- Prevent the occurrence of SA through effective mitigations (i.e. providing water and power)
- Arrest SA within the reactor core vessel (i.e. preclude the generation of Hydrogen gas and Carbon Monoxide - generated from reactor core with the concrete interaction.)
- Protect the integrity of the containment building and limit the release of fission products

Accident progression differ based on the reactor type and design. For example, in CANDU fleet reactors, the accident progression is initiated when total loss of AC occurs (due to BDBE or any other reason). Control of reactor core is established by activating the SDS1

(shut-off rods) and/or SDS2 (Boron injection) emergency systems to stop core reactivity. Although reactivity within the core is assumed stopped, the decay heat (estimated 6-7% of total reactor core thermal power) immediately after shutdown continues to be produced. Heat sink is immediately required:

- The first heat sink in CANDU is the secondary heat transport system - steam generator water inventory and other passive inventories.
- The Second heat sink is the primary Heat Transport System (HTS) - moderator inventory
- The third heat sink is the shield tank water inventory
- In the event the accident progression is not arrested due to lake of adequate heat sink the accident progresses to Severe Accident domain where further Severe Accident Management Guidelines (SAMGs) and protocols will be in place to manage the accident with primary attention to:
  i. Management and mitigation of Hydrogen production
  ii. Containment venting and mitigation of integrity challenges

Accident progression in other reactor design such as BWR and PWR is comparable to CANDU.

1.3 Current evaluation of CCF due to BDBE

The Fukushima accident caused major environmental and economical loss. However, unlike earlier nuclear accidents, the Fukushima accident was due to a Beyond Design Basis Event (BDBE). Most of current operating NPPs in the world are designed to meet only design basis

accidents. As a result, BDBE became a major concern in the nuclear industry and major modification projects are under way worldwide to fill this gap.

In addition to these modification projects, NPPs are re-evaluating their safety and probabilistic risk assessments (PRA) for both internal and external hazards to include BDBE. Common Cause Failures (CCF) models are used in PRA however capturing true impact of BDBE into the model continue to be a challenge for the following reasons:

- dependent probability failures due BDBE database are not available. Common approach by NPPs to overcome this issue via:
    1. Treating external event (i.e. external flood or fire) as an initiating event in PRA modeling.
    2. Assign a common cause failure multiplier factor (for components) to account for dependent failure. This multiplier is purely subjective and relies on the expert experience and not on extensive data/statistics.
- The CCF models used in PRA are not developed with event and condition assessment in mind. As a result, many issues arise with PRA models in their application to BDBE assessment since:
    1. CCF models are not causal (i.e. Beta model)
    2. CCF models apply symmetry assumption (i.e. BPM model)
    3. CCF models are not modeled across component or system boundaries
    4. CFF Impact on more than one failure mode not captured

These gaps prohibit to capture and to truly quantify the safety risk due to BDBE in PRA assessment.

1.4 Emergency Preparedness Status: Problem Statement

Currently, NPPs do not have a metric to gauge their emergency/mitigation readiness nor a method for quantifying NPPs' Vulnerability. The need for such a metric stems from:

- the inadequacy of current NPPs design safety to mitigate effectively accidents due to BDBE (such as Fukushima)
- PRA analysis tool does not account accurately for BDBE impact due to limitation within CCF models applied

A need for an objective and practical method to assist NPPs to measure their mitigation readiness and NPP vulnerability due to BDBEs is pending. In an attempt to fill this gap, a model and assessment method is derived to encompass lessons learned (primarily) from the Fukushima accident. *Emergency Mitigation Preparedness (EMP)* model is developed and illustrated in this thesis. The EMP model can quantify mitigation readiness and NPP vulnerability due to single or multiple BDBEs (external/internal events). EMP method is not a statistical or probabilistic approach and therefore it does not require expert advice to determine the model's factors nor does it depends on extensive equipment reliability database (as the case for parametric models - to be discussed later in Chapter 3).

The EMP model is founded on four pillars: (1) applicable emergency equipment capable to mitigate severe accidents (2) NPPs' built-in active and passive safety features to mitigate severe accidents (3) continuous improvement of human reliability factors and safety culture and (4) adequate physical barriers in the NPP.

1.5 Summary

The inadequacy of current NPPs design safety to mitigate effectively accidents due to BDBE (such as Fukushima accident) and the inability of the PRA analysis tools to account accurately for BDBE impact (due to limitations within the CCF models) limit the NPPs to design an effective emergency mitigation plan to (1) cool the reactor (2) contain the reactor and (3) safely arrest any potential accident progression due to BDBE/external events.

This gap is challenged in this paper and Emergency Mitigation Preparedness (EMP) model and assessment is developed to meet the above three criteria. It will be shown (in chapter 5) how the EMP will provide a quantitative assessment to the NPP's emergency mitigation preparedness and an overall NPP vulnerability due to BDBE (or external events). During the EMP evaluation process, potential gaps within the NPP will be determined and potential opportunities to improve emergency mitigation readiness and consequently the NPP vulnerability due to BDBEs are identified. The execution of the EMP assessment will provide the NPP operators and shareholders current emergency mitigation readiness and NPP vulnerability due to beyond design basis events or external events. Emergency mitigation readiness status is considered a significant input factor in the informed emergency risk analysis process that can contribute to a safer NPP operation and a higher protection to the public, environment and economy.

Chapter 2

Regulatory Guidance for External Events - IAEA Safety Standards

2.1 Introduction

The International Atomic Energy Agency (IAEA) is founded in 1957 on principal objectives such as to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world. The terms of Article III of the agency's Statute state the IAEA is authorized to establish standards of safety for protection against ionizing radiation as well as to provide member states for the application of these standards to peaceful nuclear activities. With no bias intended, this thesis will use IAEA standards for discussion. It is worthy to note that IAEA's safety standards are also mirrored by other international organizations such as WANO and INPO. IAEA standards are not legally binding by Member States but may be adopted for use in their national regulations and laws to encompass their own nuclear program. For instance, the Canadian Nuclear Safety Commission (CNSC) is the federal regulator and licensing body in Canada where much of safety regulations such as S-294 that deal with PRA analysis in Canadian NPP safety is administered and enforced. The U.S. Nuclear Regulatory Commission (NRC), on the other hand, is the federal regulating body in the United States. The NRC is known to be more aggressive in passing regulations to govern the nuclear operators in the US; in fact, the NRC Regulations 10 CFR Part 50 Domestic Licensing of Production and Utilization Facilities (which govern the nuclear plants licensing and operation in America) is part of U.S. Federal Law.

IAEA establishes and issues many safety standards series for the purpose to share up-to-date knowledge in nuclear advancement and in design for protections and safety of NPP with member states. Furthermore, IAEA issues numerous Safety Guide publications which provide design standards against different types of EEs. IAEA provides recommendations and guidance on design for the protection of nuclear power plants from the effects of external events. By definition, External Events (EE) are events that originate either off NPP's site or within the boundaries of the site but from sources that are not directly involved in the operational states of the NPP units. Source of External Events can be from Natural forces (i.e. floods) or human induced activity (i.e. aircraft crash). Significant events, both as design basis external human/natural induced events must be identified and selected as design basis external events (DBEEs) in the preliminary phases of the site evaluation process. Typical list of human induced events are as follows [1]:

a) Aircraft crashes
b) Explosions with or without fire originating from off-site and on-site sources
c) Release of hazardous gases (toxic) from off-site and on-site storage
d) Release of radioactive material from off-site sources
e) Release of corrosive gases and liquids from off-site and on-site storage
f) Fire generated from off-site sources
g) Collision of ships or floating debris with accessible safety related structures
h) Collision of vehicles at the site with system, structure and components (SSCs)
i) Electromagnetic interference from off the site (e.g. from communication centres) and on the site (e.g. from the activation of high voltage electric switch)

Furthermore, typical list of Natural Events include the following [1]:

- Extreme meteorological conditions (snow, hail, frost, freezing and drought)
- Floods (e.g. due to tides, tsunamis, precipitation and dam failures)
- Tsunami/Cyclones (hurricanes, tornadoes and tropical typhoons)
- Abrasive dust and sand storms
- Lightning
- Volcanism
- Seismic/Earthquake
- Collision of floating debris (ice, logs) with accessible safety related structures

2.2 IAEA External Event Design Requirements for NPP

The IAEA adopts design requirements for NPP in External Events situations to ensure that the overall safety concept of defence in depth is maintained and the design shall prevent as far as practicable [2]:

- Challenges to the integrity of physical barriers
- Failure of a barrier when challenged
- Failure of a barrier as a consequence of failure of another barrier

In sum, all levels of defence in the NPP shall be available at all times to protect NPP in EE situations. The IAEA agency, in an effort to emphasize safety planning in systems, structures and components (SSCs) within the nuclear site, categorized items into the following [2]:

I. External event Category 1 (EE-C1): Items whose functioning should be always maintained in the event of the DBEE. Also, EE-C1 includes items required for preventing or mitigating plant accident conditions for a long period. Typical EE-C1 systems are:

- The reactor system containment structure (including foundations) or the external shielding structure
- The structures supporting, housing or protecting items important to safety, to the extent necessary to ensure their functionality
- Structures protecting the plant from external events
- The power and instrumentation and control (I&C) cables relevant to safety related items
- The control room or the supplementary control points, including all equipment necessary to maintain the control room or supplementary control points within safe habitability limits for personnel and safe environmental limits for equipment protected against DBEEs
- Systems or portions of systems that are required for monitoring, actuating and operating those parts of systems protected against DBEEs
- The emergency power supplies and their auxiliary systems necessary for the active safety functions
- The post-accident monitoring system.

II. External event Category 2 (EE-C2): Items whose loss of functionality may be permitted as long as it does not limit or impair the functionality of EE–C1 items in the event of a DBEE. Typical systems that are classified as EE-C2 are:

- SSCs whose continued functionality is not required but whose failure could reduce the functional capability of any plant features specified above (EE-C1) to an unacceptable safety level or could result in incapacitating injury to occupants of the control room who are necessary to perform a safety function

III. External event Category 3 (EE-C3): Items that are parts of systems that may generate events with radiological consequences different from those generated by the reactor (e.g. spent fuel building and radioactive waste building). Typical systems that should be classified as EE-C3 are:

- SSCs for spent fuel confinement
- Spent fuel cooling systems
- Systems for the containment of highly radioactive waste in all forms

IV. External event, non-classified (EE-NC): All other items.

In this thesis we will only discuss the IAEA safety standards to those areas of External Fire, Floods, Extreme Winds, Tsunami, Ice Storms/Extreme low temperature in accordance to this study's objective.

2.3 External Fire:

2.3.1 IAEA Standards [1]

External Fire events originate outside the nuclear site from potentially numerous sources such as: fuel storage, vehicles, nearby forest, ignited fuel from aircraft crash. External Fire events have significant impact on safety of NPP safety and as a result, the IAEA issued standards to protect NPP against them by having:

- Physical Barriers

During the initial NPP site approval process, precautionary measures should be taken to reduce the amount of combustibles around the NPP and its main access routes. Coastal nuclear sites, furthermore, should consider physical barrier from potential burning oil spilled into the sea. Similarly, sites nearby flight path should be protected from air crashes at NPP site that might result in igniting plane's fuel. Barriers to external fires may include removal of nearby trees/vegetation that could propagate a fire and/or developing physical barriers/zones to contain external fire from NPP.

- Durable Site Structure

The design of NPP should withstand and/or prevent smoke or heat generated by external fire from damaging the safety functions and/or from limiting the stability of safety related structures at the site. The site buildings integrity should be intact against the heat flux and potential damage caused by External Fire.

- General Fire Protection

When an external fire propagates at the site or when a fire is originated at the site but outside the safety related buildings (such as from a transformer, fuel storage or a vehicle at the site), general fire protection measures should be taken. Special equipment such as foam generators and entrenching tools as well as specially trained on-site and off-site fire fighting personnel may be used to prevent such fires from penetrating structures containing items important to safety.

- Ventilation System

The ventilation system should be designed to prevent smoke and heat from affecting redundant divisions of safety systems and causing the loss of a necessary safety function (including operator action).

- Air Supply

The plant design should ensure an adequate supply of air to all diesel generators air intakes that are required to perform necessary safety functions as well as air supply to main control room.

2.3.2 IAEA Design Methods for External Fire Events [1]

- A procedure for safety verification in the event of an External Fire in order to determine (1) the maximum heat flux arriving at the NPP buildings is important to safety and (2) to determine whether the barrier resistance provided by the building exterior skin of the building is sufficient.
- The vulnerability of the NPP structures to the thermal environments and if it would withstand such environmental conditions caused by an external fire event. The verification should be based on the capacity of the material to absorb thermal loads without exceeding the appropriate structural design criteria. Note the capacity of the concrete to resist fires is mainly based on the structure's features such as thickness and the composition of aggregates.

- The capacity of steel structures exposed to large fires is limited and therefore it should not have safety related functions. (note: reinforced steel is suitable to withstand air craft impact).
- Construction codes generally provide maximum allowable temperatures of materials. As a guideline, the allowable temperature for reinforcing bars and structural steel subjected to short term (less than six hours) fires is 500°C [1].

2.3.3 Means of Protection from External Fire [1]

- Inherit Design of NPP should minimize the probability of an external fire as well as strengthen the barriers against external fires when necessary. In depth defences incorporated in the NPP design must be characterized by having redundant safety systems, physical separation by distance, by separate fire compartments or by specific barriers, and the use of fire detection and extinguishing systems should also be provided.
- If the inherent capacity of the structure is not sufficient, then additional barrier or distance separation should be added. Such as increase in the concrete thickness of the exposed structure if this enhances the structural capacity to resist other postulated loads.
- Protection of ventilation systems by isolation of the systems from outside air by means of dampers. Also there should be a separation of the inlet and exhaust hoods of one ventilation system serving one safety system from the inlet and exhaust hoods serving other redundant safety systems.

- The NPP design should ensure an adequate supply of air to all diesel generators required to perform necessary safety functions in the event of an external fire. This is achievable by separating the air intakes and separating them by distance. This is also applicable to safety related instrumentation and control systems that are vulnerable to smoke and dust
- Ability to clear roads and off-shore access by heavy equipment if necessary.
- Emergency power supply plane should be in place in event of loss of AC power and the onsite diesel generator power.
- Multiple and better Fire detection and extinguishing systems to ensure a safe shutdown manner.
- Control room may malfunction without ventilation system for 4-6 hrs. Emergency planning should be in place to provide adequate clean air in order to operate safety equipment.
- Establish early warning system and safety procedures
- Ensure emergency power supply is accessible by either on-site or off-site diesel generators.

2.4 Floods

➢ 2.4.1 IAEA Standards

Flooding scenarios in NPP induce a transient in water level at the site, static effects (water weight) and dynamic effects (from water, debris and ice). Floods can be a result of one (or a combination) of the following events [1]:

- Rain precipitation
- Runoff of water from off-site precipitation
- Snow melting
- Failure of water retaining structures (hydrological, seismic and from faulty operation)
- Failure of natural obstruction created by landslides, ice, log or debris jams and volcanism
- Sliding of avalanches and/or landslides into water bodies
- Rising of upstream water level due to stream obstructions (see scenarios above)
- Changes in the natural channel for a river
- Storm surge due to tropical or extra-tropical cyclones
- Tsunami
- Seiche, also combined with high tides
- Wind induced waves

IAEA NPP safety design standards require the following steps to combat flooding scenarios:

- Construction of external barriers, natural or artificial plant islands
- Initial site evaluation should include any site improvement (i.e. dam structures, artificial hills) to limit the effects of floods in NPP; consequently, this can affect the design basis for the plant
- Establishing 'incorporated barriers' which are directly connected with the plant structures (special retaining walls and penetration closures) [1]

- Increase measures for site protection and increase reliability of drainage systems and the functionality of safety related equipment
- In-leakage is directly a result of poor sealing in structural joints or cable conduits and inspection openings. Therefore, NPP design should limit or eliminate these design faults.
- If external barriers and natural or artificial plant islands are part of the site protection system, the design basis flood for the site affects primarily the site protection structures and the water intake structures
- As an additional measure against site flooding from off-site sources should be considered and the protection of the plant against extreme hydrological phenomena should be augmented by waterproofing and by the appropriate design of all items necessary to ensure the capability to shut down the reactor and to maintain it in a safe shutdown manner.
- Identify flood causes for each plant site and place operational procedures such that real time monitoring data for the flood causes are tracked. This will enable the NPP to have a warning system to shut down the reactor core safely in the event of potential flooding
- Design all safety systems including warning systems to withstand flood, and flood secondary events such as high wind and landslide
- Proper site structure-pressure evaluation to determine whether the site will be capable to withstand static and dynamic forces and effects of floods; such as the evaluation effects of ice and debris carried by the flood and the waves
- NPP sites sensitive to precipitation should have reliable and a marginally safe drainage system

- Floods secondary products such as sedimentation, modification of water salinity, erosion, blockage of intakes (by ice or debris) and mud suspension in water should be included in the design basis evaluation and procedures to deal with these effects put in place
- The design basis flood should be appropriately combined with all the various design basis events generating the flooding itself [3]

2.4.2 Means of Protection from Floods [1]

- Ensuring both active and passive drainage systems are adequate and site specific
- Implementing proper emergency procedures based on real time monitoring data gathering of surrounding environment as well as structural monitoring of the flood protection items. Communications should be established with any flood warning systems in the site vicinity to enable the plant to be put in a safer condition
- Establishing transport and communication routes. Based on operating experience, major risk is associated with the unavailability of transport and communication routes at the site and between the site and the surrounding areas for use in making contact with emergency teams, the turnover of operator shifts and the provision of information to the public. Availability of communication routes is a key part of the emergency planning
- Construction of external barriers, natural or artificial islands
- Active and passive barriers should be incorporated in the site structures directly (retaining walls, penetration closures)

- Improve drainage system reliability and functionality and increase their safety margin to withstand heavy precipitation
- Implement Active and passive drainage system in site design and ensure they are adequate for site specific. (i.e. automatic flood gate that utilizes the hydrostatic force of water to engage the gate; similarly, vent shaft system that will shut down the vent in event if high road is flooded and protect sensitive underground equipment such as transformers..etc)
- Improve sealing in structural joints or cable conduits and inspection opening, to limit in-leakage into site structures
- Identify flood causes for each plant site and place operational procedures such that real time monitoring data for the flood causes are tracked. This will enable the NPP to have a warning system to shut down the reactor core safely in the event of potential flooding.
- Design all safety systems including warning systems to withstand flood, and flood secondary events such as high wind and landslide
- Structures should withstand both static and dynamic forces of floods (such as effects of ice, water, debris carried by flood and waves)
- Site design must deal with secondary flood effect: sedimentation, modification of water salinity, erosion, blockage of intakes (by ice or debris) and mud suspension in water
- Emergency power supply plan should be in place in the event of loss of AC power and the onsite diesel generator power

- Loss of cooling tower: alternatively a different method of providing cooling water to the plant could be provided, for example from a different source or by a closed loop air cooled system
- Real time monitoring of flood causes and establishing warning system
- Ability to clear roads and off-shore access by heavy equipment if necessary
- Ensure emergency power supply is accessible by either on-site or off-site diesel generators

2.5 Extreme Winds

Tropical cyclone, Typhoon, Hurricanes and Tornadoes are considered part of the Extreme Winds events affecting NPP safety. A tropical cyclone is described as a warm core, large scale circulation of winds around a central region of low atmospheric pressure. Hurricanes are considered tropical cyclones occurring in the Atlantic Ocean, the Caribbean Sea, the Gulf of Mexico and the eastern Pacific Ocean. Whereas, Typhoons are tropical cyclones experienced in the west Pacific. Tropical cyclones can produce extremely powerful winds and torrential rain, as well as high waves and storm surges. On the other hand, Tornadoes are generally described as violently rotating columns of air, usually associated with a thunderstorm [4].

➢ 2.5.1 IAEA Standards [1]

- NPP site should adhere to References [5] which provide guidance for a site specific review of the potential risk of extreme winds (i.e. typhoons, hurricanes, cyclones, tornadoes)

- Extreme winds in NPP could damage and/or affect the power supply to the site. Furthermore, potential damage to switchyards is probable causing turbine trip and loss of off-site power. NPP sites close to the marine environment are sensitive to a heavy salt spray from the sea in the form of a precipitation which could damage exposed electrical equipment and cause corrosion and malfunction
- High winds have been known to cause collapse of cooling towers as a consequence of a 'group effect', while they are individually designed to withstand an even higher wind speed

2.5.2 Means of Protection from Extreme Winds [1]

- Protection from Extreme winds carrying moisture which may cause flooding. Similarly, extreme winds can cause destruction of structures, surfaces and equipments when carrying dust or sand
- Extreme winds can give rise to high local pressure gradients and also to missiles that could affect the performance of cooling towers
- The UHS transport systems should be examined to ensure that any changes in water level caused by an extreme wind cannot prevent the transport and absorption of residual heat
- The interaction effects from wind on safety related structures could be of concern: heavy and high rising cranes parked outside the containment might fall over, as well as chimneys and cooling towers. A site specific analysis should be performed to determine degree of hazard

- NPP may be exposed to salt sprays from the sea in the form of a precipitation which will damage exposed electrical equipment and cause corrosion and malfunction. Protection of exposed system is required
- Ability to clear roads and off-shore access by heavy equipment if necessary
- Protection of cooling tower from airborne objects, if possible
- Erection of physical barriers to protect site structure, water intakes and UHS structures from damage caused object (ship) missiles collision, ice or floating debris
- Establish early warning system and safety procedures
- Ensure emergency power supply is accessible by either on-site or off-site EDGs

2.6 Ice Storms/Extreme Low Temperature [1]

Ice Storm features freezing rain which is a precipitation that falls when the temperature on and above surfaces is below freezing. The drops became super cooled and freeze upon impact with soil or with any surface, resulting in the formation of a layer of ice. In NPP, ice due to freezing rain and snow is known to cause increase in the dead loads and the response of site structures, specifically, there is significant increases in the static and dynamic response to wind action for conductors in transmission lines. Also, formation of ice in cooling systems may affect their overall efficiency. Ice Storms may also affect AC power on site and the grid in general.

➢ 2.6.1 Means of Protection from Ice Storm/Extreme Low Temperature

- In efforts to prepare NPP site against extreme temperature/Ice Storm hazards, IAEA issued a reference [5] which gives guidance for a site specific review. Most of these hazards affect very specific plant systems such as:

a) The availability of the UHS [6] which is mainly affected by ice

b) The availability of off-site power [7] which is mainly affected by wind, ice, snow, frost and lightning

c) The functionality of safety related equipment, and particularly the I&C equipment [8] which is mainly affected by temperature, moisture and lightning

- Extreme low temperature can be the root cause of many malfunctions in NPPs such as:

a) Affecting I&C systems and producing false and erratic signals

b) Low temperatures have at times created moisture condensation in closed rooms, with consequent dropping of water onto electrical equipment causing short circuits and malfunctions

c) Low temperatures have also prevented the air ventilation system of some NPPs from working properly

d) Low temperature may affect the operation of diesel generators where the fuel can show separation of paraffin

e) Low temperature may damage the external power supply system and limit the availability of service water

- Snow/Ice induced damage is usually represented by the unavailability of the power supply or the electrical grid, but snow could also affect ventilation intakes and discharges, structural loading, access by the operator to external safety related facilities and mobility of emergency vehicles.

- Intake structures for the heat transport systems directly associated with the UHS should be designed to provide an adequate flow of cooling water during seasonal water level fluctuation
- Due allowance should be made for the effects of extreme cold weather conditions on make-up supplies
- Measures should be taken, by testing and/or analyzing to confirm that the facilities provided to reject heat to the UHS still retain their capability under extreme meteorological conditions. Such as, for example, monitoring the operability of spray nozzles to check that they do not become frozen or intake screens blocked by ice
- Alternative path(s) for water cooling should be provided to counter the formation of frazil ice at the service water intake, if justified by site conditions. In this case, provision should be made for adequate instrumentation and alarms and relevant procedures and training
- Establish early warning system and safety procedures
- Ensure emergency power supply is accessible by either on-site or off-site EDGs

2.7 Tsunami

A tsunami is a series of travelling waves generated by deformation or disturbances of the sea floor such as: Earthquakes, volcanic activities, underwater and coastal landslides. For example, in Deep Ocean, tsunami wave speeds could exceed 800 km/h, with a wave height generally less than a few tens of centimetres, and in the case of an earthquake source with wave lengths often exceeding 100 km. When the tsunami waves reach the coastal zone, the wave speed is

reduced and wave length is shortened when the depth decreases, however, tsunami waves become steeper and increase in height on approaching shallow water [4].

Tsunamis can also be classified as 'local' tsunamis or 'distant' tsunamis. A tsunami is called a local tsunami when it affects only the region near its source. Distant tsunami is less frequent but affecting wider regions and travels across the ocean or sea to arrive at places distant from their source. Since tsunami is a combination of an Extreme Flood and Extreme Wind event, site recommendation to protect against such an event is the sum of both Extreme Flood and Extreme Wind recommendations (see above).

2.8 Summary

This chapter summarized the IAEA standards for nuclear plant design facing External Events such as: External Flood (refer to Appendix A for detailed summary), External Fire (refer to Appendix B), Extreme Wind (refer to Appendix C), Snow Storm (refer to Appendix D) and Tsunami. Other member states have passed further top level regulations to their local nuclear operators to address potential damage and threat caused by EE to reactor core, reactor safety equipment and site's main functional areas and equipment.

Along with implementing safety regulations, NPPs are required to investigate potential successful chain of events leading to severe accidents scenarios. Next chapter will discuss parametric models currently employed in Probabilistic Risk Assessment (PRA) and used in the nuclear industry to assess safety-hazard in NPP . The emphasis will be on the importance of Common Cause Failures (CCF) in evaluating component (dependent) failure rate and on the parametric models' properties and limitations.

Chapter 3

Common Cause Failures & Parametric Models

3.1 Introduction

Component failures are divided into independent failures (i.e. failure to start) and dependent failures due to common cause failures. A common cause is an event or mechanism that can cause two or more failures (basic events) to occur simultaneously due to various underlying causes such as External Events (EEs). The failures resulting from the common cause are called common cause failures (CCFs) and/or dependent failures. Because common causes can induce the failure of multiple components, they have the potential to increase system failure probabilities. Thus, the elimination of common causes can appreciably improve system reliability.

Equipment reliability and availability for plant operators are paramount in order to maximize plant efficiency, productivity, profitability and safety. As a result, quantifying equipment and component failures more accurately to include CCF (in addition to independent failures) will result in a better comprehension of total system failure, how to protect equipment failure and how to mitigate equipment failure consequences.

In risk, safety and reliability industries, various parametric models are used which evaluate CCF when applying Probabilistic Risk Assessment (PRA) analyses. Most common and current applied models internationally are: Binomial Failure Rate model (BFR), Beta-Factor model (BF), Alpha-Factor model (AF), Multiple Greek Letter model (MGL). The inception of Probabilistic Risk Assessment (PRA) analysis came from the aerospace industry in the 1960s with the

development of Fault Tree Analysis (FTA) in 1961 by Bell Laboratories for the Minuteman Launch Control System [9]. In the 1970s, with the number of Nuclear Power Plants (NPP) spreading geometrically, the safety of NPP became an important policy issue. The nuclear industry borrowed the techniques used in the aerospace industry to perform PRA and significantly contributed to further developing these techniques. With the publication of WASH-1400 in 1975, event trees become a part of the PRA as well as the concept of the common mode failure (CCF) [9].

Probabilistic Risk Assessment (PRA) analysis quantifies the risks inherent within a given engineered system; the PRA analysis conclusion determines *not how safe is the system but rather how unsafe is the system*. PRA can potentially contribute to enhancement to the design and operating phases of the system or plant. There are three PRA levels of analysis addressing different aspects of accidents in NPPs [15]:

- Level 1 PRA analysis models the responses of NPPs (including their operators) to initiating events that challenge plant operation. These models identify accident sequences that result in damage to the reactor core.
- Level 2 PRA models and analyzes the progression of "severe accidents" by considering how the reactor coolant and other relevant systems and the containment respond to the accident.
- Level 3 PRA models the release and transport of radioactive material in a severe accident and estimates the health consequences and economic impact: (1) early fatalities and injuries and potential cancer fatalities resulting from the radiation doses to

the surrounding population and (2) economic costs associated with evacuation, relocation, property loss, and decontamination.

In sum, having the Level 1, Level 2 and Level 3 PRA results, it is then possible to estimate the NPP's safety risk (event likelihood × consequences) to the public. In preparation to protect against consequences from external events and/or severe accidents, a thorough and adequate mitigation plan must be ready to address potential hazards the site may experience and protect the NPP, public and the environment.

PRA analysis can be used to assess the strengths and weaknesses in a given design as well as assess the system responsiveness and sensitivity of the risk to certain design or performance assumptions. This is done by relating the engineered system risk to the factors that contribute to the risk such as operator reliability, equipment reliability, or plant operating or maintenance procedures. Finally, PRA analysis is often used as an input in the risk-informed decision making process such that the maximum benefit from design, construction or maintenance activities can be achieved.

3.2 Failure Modes & Root Causes

In PRA, the *frequency and probability* of failure associated to a given component are the values often used in PRA analysis. These data are typically found in well established databases that hold historical failure probabilities and event frequencies (event per unit time) of a given component or event that was accumulated from the industries at large over the years (from nuclear, manufacturing, chemical or processing industrial plants). Defined as a measurement of uncertainty, probability is a unit less quantity and ranges between 0 and 1. In PRA analysis, the

probability value is usually used to characterise component's failure(s). Furthermore, initiating events are normally expressed as frequencies (for instance the frequency of a loss of offsite power or external flooding) which are often converted to a probability value before the PRA analysis is executed.

Component failure event modes or probabilities are categorized into: failure to start (run), failure to continue to run, or functional/structural failure. Failure modes for each equipment are identified and modelled such that the overall failure (or unavailability) of that piece of equipment or component can be identified and there are a number of probability models based on failures. Typical probability models are binomial, Poisson, normal or log-normal. These models convert given frequency information into probability values. These models classify failure events or modes into four main categories such as *Functional Failures, Common Cause Failures, Demand Failures and Run Failures*:

- ***Functional Failures*** are failures where the system may respond passively and or the inability of the component or system to fulfil one or more of its functions.

- A single initiating event that results in the failure of multiple components or systems is termed a ***Common Cause Failure***. An example of ***internal*** common cause failures would be moisture presence, due to steam line rupture, that affects the function of nearby components; or ***external*** common cause failures like seismic activity (i.e. earthquakes) causing mass equipment failure.
- ***Demand Failures*** are defined when an equipment fails to start (i.e. in a case of a valve, it is failure demand is the failure to open or close). In NPP, typical systems under this category that experience demand failures would be Auxiliary Feed-water pumps,

Shutdown Cooling system, and Emergency Power. Demand Failure can be represented by the Binomial Distribution, such as follows:

$$P\{\, r \;\; failures\ in\ N\ trials \mid p \,\} = \binom{N}{r} * \; p^r * (1-p)^{N-r} \qquad (3.1)$$

where,

P = the Probability of failure for a single demand,

p = number of failures/number of demands, and

$\binom{N}{r}$ = is the r-out-of-N combinations = $\frac{N!}{(N-r)!r!}$

Equation (3.1) can be used to convert frequencies of component demand failures to probabilities when conducting PRA analysis. The probability of failure for a single demand then would just be quantified to be "P".

- ***Run Failure*** is defined as an equipment that fails to run after a certain time (i.e. failure to ***run continu***ously or after some initiating event). These types of failures are time-related or time-dependent. For instance, emergency feed-pump is a typical system which is prone to run failure. Time related *Run Failure* is represented by the Poisson distribution such as:

$$P\{\, r \;\; failures\ in\ (0,t) \mid \lambda \,\} = \frac{(\lambda t)^r * e^{-\lambda t}}{\lambda!} \qquad (3.2)$$

where,

P = the Probability of failure for component

λ = failure rate per unit time

t = required operational time (mission time)

In shared component or system failure event, shared failure cause is an indication of a **root cause** and **coupling mechanism** between components. There are four broad types of root causes: hardware equipment failure, human error during operation, environmental stress applied to components, and external events that cause environmental effects [10].

The *root cause* is identified as the most basic cause of component failure which, if corrected, would prevent reoccurrence of the cause. Root causes are categorized into hardware, human, environmental and external, while Proximate *causes* are defined as a characterization of the failure condition that led to the failure. The proximate cause can be regarded as a symptom of the failure cause and does not necessarily provide a complete understanding of what led to that failed condition. Potential proximate causes are found in component or system design, construction, installation, manufacture inadequacy, operational, human error, internal environmental causes, external environmental causes.

Coupling mechanism, on the other hand, implicates the condition for multiple components to be affected by the same cause. These coupling mechanisms can be hardware-related, maintenance related, operation related, location, environment related, data based, plant configuration related, etc. It should be pointed out that there is an *intrinsic dependency* between components where the functional status of a component is affected by the functional status of other components; this can be further categorized into (1) functional requirement dependency (2) functional input dependency and (3) cascading failure. On the other hand, *Extrinsic dependency* is a situation where the dependency or coupling is not inherent or intended in the functional characteristics of the system. Extrinsic dependencies may be related to (1) Physical or environment stresses or (2) human intervention [11].

3.3 Common Cause Failures

Common cause failures (CCF) event is an event associated to a failure or degradation of one or multiple components, simultaneously or within a short period, due to a shared dependency such as External Events which could affect multiple components and systems at once (i.e. 2011 Tsunami – Fukushima accident, Japan) . This shared dependency addresses the fact that a shared cause must exist in order for a common cause failure (CCF) of two or multiple components to occur. The Nuclear industry defines CCF as a dependent failure in which two or more component fault states exist simultaneously or within a short time interval, and are a direct result of a shared cause. To illustrate the significance of CCF in failure risk evaluation for a given engineered system, consider a common redundancy system design in NPP such as *two-out-three* system (see figure 3.1). In the nuclear industry, redundancy is a typical defence strategy to increase the system's reliability. The considered system (2 *out of* 3) will fail if two or more components fail. Considering the first case where three components can only fail *independently*. Let the failure probability of each component be denoted by the component name with a subscript "ind" such as

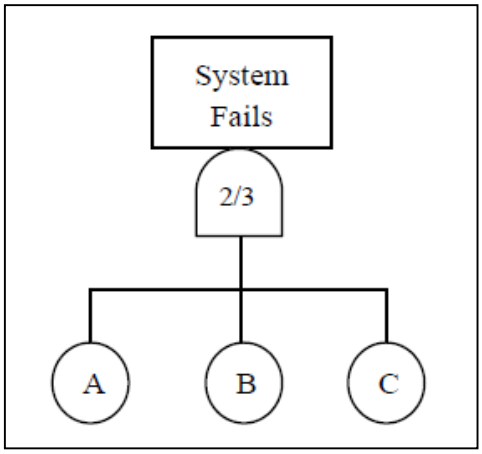

Figure 3.1: Independent failure for 2-out-3 system

A_{ind} , B_{ind} , C_{ind} . Therefore, the total system's failure probability expressed in Boolean logic is:

$$P_{ind}(\text{system}) = (A_{ind} * B_{ind}) + (A_{ind} * C_{ind}) + (B_{ind} * C_{ind}) + (A_{ind} * B_{ind} * C_{ind}) \quad (3.3)$$

Now, let's consider the case where the system failure may also be due to simultaneously or dependent component failures. Let C denote common cause failure and subscript denote the component involved in the failure event such as C_{AB}, C_{AC}, C_{BC}. The System failure for 2-out-3 system is illustrated by figure 3.2 below:

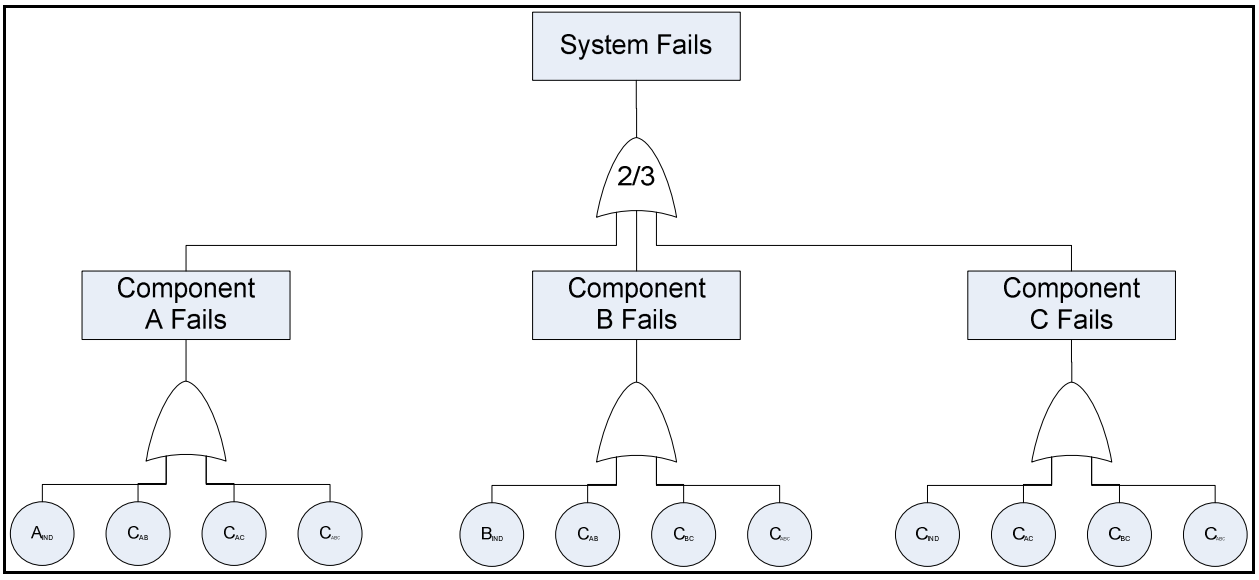

Figure 3.2: CCF & independent failure for 2-out-3 system

The Boolean logic representation of the component (A) failure frequency is as follows:

$$P(A) = P_{ind}(A) + (C_{AB}) + (C_{AC}) + (C_{ABC})$$

Total Comp. (A) failure = Comp. (A) Independent failure + Comp.(A) failure due to CCF

(3.4a)

And, the Boolean logic representation of the component (B) failure frequency is as follows:

$$P(B) = P_{ind}(B) + (C_{AB}) + (C_{BC}) + (C_{ABC})$$

Total Comp. (B) failure = Comp. (B) Independent failure + Comp.(B) failure due to CCF

(3.4b)

And, the Boolean logic representation of the component (C) failure frequency is as follows:

$$P(C) = P_{ind}(C) + (C_{AC}) + (C_{BC}) + (C_{ABC})$$

Total Comp. (C) failure = Comp. (C) Independent failure + Comp.(C) failure due to CCF

(3.4c)

It can be shown, that the reduced Boolean representation of the total system failure is:

$$P(\text{system}) = A_{ind}*B_{ind} + A_{ind}*C_{ind} + B_{ind}*C_{ind} + C_{AB} + C_{AC} + C_{BC} + C_{ABC} \quad (3.5)$$

Comparing equations (3.5) to equation (3.3) shows clearly the contribution of CCF component failures events in estimating the overall system reliability. As a result, the importance of multiple component failures due to CCF in quantifying system's availability must not be ignored if a plant's true safety and availability is desired.

Common cause failures analysis is currently handled in risk assessment analysis by implementing ***parametric models*** such as beta factor model, alpha factor model, multiple Greek letter (MGL) model which are easy to understand and use. It is important to note that these models depend on certain assumptions and require plentiful of data (from the industry) when applied. Other models such as Unified Partial Method (UPM) are used but mostly in use in United Kingdom (and Europe) and rely heavily on expert judgement.

3.4 Parametric Models

Separation, redundancy, fail-safe design, staggered testing and maintenance, quality control and diversity are the main principles and defense strategy upon which most of the safety systems in the nuclear industry are being designed. These strategies increase system's availability and reliability. CCFs have been given a great deal of attention within the

Probabilistic Safety Assessment (PSA) and PRA analyses of nuclear power plants. There are basically two approaches for consideration of dependent failures in PRA analysis or for any system reliability analysis in general: implicit and explicit approach. The **implicit approach** is associated with modeling of multiple failure events, for which no clear root cause can be identified and treated explicitly. On the other hand, the **explicit approach** is appropriate when the CCF cause is evident and may be included in the PSA and PRA analysis [12]

The parametric models to be presented will be described by showing how each model is used to calculate the probability of occurrence of the various basic events. Numerous parametric models have been proposed, and some have been widely used in risk and reliability analyses. The two major categories are: Shock Models and Non-shock Models. The **shock models** (such as Binomial Failure Rate - BFR) recognize two failure mechanisms: (1) failures due to random independent causes of single component failures and (2) failures of one or more components due to common cause "shocks" that impact the system at a certain frequency. The **non-shock models** (such as Beta factor, MGL, alpha factor) estimate basic event probabilities without postulating a model for the underlying failure mechanisms. [10]

➢ 3.4.1 Basic Parameter Model - BPM [13]

The **basic parameter model** refers to the straightforward definition of the probabilities of the basic events. The $\boldsymbol{k^{th}}$ parameter represents a probability of a basic event involving *k* specific components $(1 \leq k \leq m)$ in a common cause component group of size *m.* The model is based on symmetry assumption that the probabilities of similar basic events involving similar types of components are the same. Failure probability ($\mathbf{Q_k}$) can be defined as demand-based (frequency

of failures per demand) or time-based (rate of failures per unit time). Q_k can be defined both for the standby failure rates as well as for the rate of failures during operation. Also (Q_k) can be calculated directly from data; however, data required are not normally available, so other models with less stringent requirements on data are used. Having in mind the assumption on symmetry, the total failure probability, *Qt*, of component in a common cause group of *m* components can be written as [13]:

$$\boldsymbol{Q_t} = \sum_{k=l}^{m} \binom{m-l}{k-l} Q_k^{(m)} \qquad 3.6$$

where the binomial term (below) represents the number of different ways that a specified component can fail :

$$\sum_{k=l}^{m} \binom{m-l}{k-l} = \frac{(m-l)!}{(m-k)!(k-l)!} \qquad 3.7$$

The basic parameter model is best explained with an example using a two-out-of-three parallel configuration of similar components (A, B, and C) (see example in pages 6-8).

➢ 3.4.2 Beta Factor Model [14]

The **beta factor model** is a single parameter model which utilizes one parameter in addition to the total component failure probability to calculate the common cause failure probabilities. Originated by Fleming K.N. (1974), the Beta factor models is considered the earliest and most commonly used parametric model used in treatment of common cause failures (CCF) in applied risk and reliability analysis. Main advantages of this model include simplicity, dependence on small number of parameters (only one parameter - Beta) and being conservative relative to other parametric models; however, Beta-factor model does not reward different levels of redundancy. The limitation of this model lies within its model assumptions. The beta factor

model assumes (1) that a constant fraction (β) of the component failure rate can be associated with common cause events shared by other components in that group. The second (2) assumption is that whenever a common cause event occurs, all components within the **common cause component group (CCCG)** are assumed to fail. This assumption of a complete coupling between redundant units, in Beta factor model, means that the occurrence of a common cause will lead to total failure of all redundant units in a given system. Therefore, for a group of m-components, all k-failure components, Q_k $(2 \leq k \leq m)$ are zero except Q_1 and Q_m . Therefore, using the beta factor model, in a common cause group of m-components, we have:

$Q_k = (1- \beta)*Q_t$ ------- for k=l 3.8

$Q_k = 0$ ------- for $2 \leq k <$m 3.9

$Q_k = \beta*Q_t$ ------- for k=m 3.10

From the equations above, it can also be shown that $\beta = \frac{Q_m}{Q_1 + Q_m}$

(Q_t, the total failure probability of one component, is given as: $Qt = Q_1 + Q_m$)

According to The Electric Power Research Institute (EPRI), the failure rate for more than two components can be extended only for pumps, valves and diesel generators, such as:

$$\beta_k = \beta_2 * \frac{FR_k}{FR_2} \quad 3.11$$

where:

β_k = Beta factor for the k-components (not k^{th} component),

β_2 = Beta factor for two components (from NP-3967);

FR_k = Failure rate for "k" components from appropriate NUREG/CR report (78,79,80)

FR_2 = Failure rate for two components from appropriate NUREG/CR report (78,79,80)

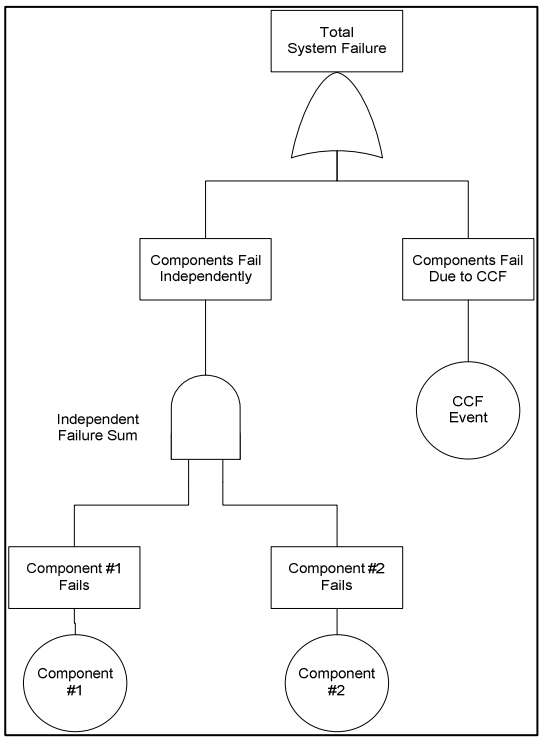

Figure 3.3: Modeling system failures: independent and CCF failures

The beta factor model requires (1) an estimate of the total failure rate of the components, which is generally available from generic data sources (i.e. Licensee event report - LER), and (2) a corresponding estimate for the beta factor. The estimators of beta do not explicitly depend on system or component success data, which are not generally available. Also, estimates of the beta parameter for different types of components do not vary considerably. These two observations and the simplicity of the model are the main reasons for its wide use in risk and reliability studies. In sum, the Beta factor is considered conservative, not causal, transferable (between similar type of equipment), however not consistent with data.

➢ 3.4.3 Multiple Greek Letter (MGL) Model [10]

The MGL model is an extension of the beta-factor model. The MGL model was the one used most frequently in the International Common Cause Failure Reliability Benchmark Exercise [10]. In the MGL model other parameters (ϒ & δ) in addition to the beta (β) factor are introduced to account more explicitly for higher order redundancies and to allow for different probabilities of failures of subgroups of the common cause component group (thus overcoming the limitation found in beta factor model discussed earlier in Beta-Factor model). The MGL parameters consist of the total component failure probability, Q_t, which includes the effects of all independent and common cause contributions to that component failure, and a set of failure fractions, which are used to quantify the conditional probabilities of all the possible ways a common cause failure of a component can be shared with other components in the same group, given component failure has occurred. For a group of (m) redundant components and for each given failure mode, (m) different parameters are defined. For example, the first four parameters of the MGL model are: $\mathbf{Q_t}$ is the total failure probability of each component due to all independent and common cause events. Factor (**β)** is conditional probability that the cause of a component failure will be shared by one or more additional components, given that a specific component has failed. The factor (**ϒ)** is the conditional probability that the cause of a component failure that is shared by one or more components will be shared by two or more additional components, given that two specific components have failed. And finally, (**δ)** factor is the conditional probability that the cause of a component failure that is shared by two or more components will be shared by three or more additional components, given that three specific components have failed.

The general equation that experesses the probability of (k) specific component failures due to common cause, Q_k , in terms of the MGL parameters, is consistent with the above definitions. The MGL parameters are also defined in terms of the basic parameters. In the case of a group of three similar components, the relation between MGL paramaters expressed in basic parameters are as follows:

$$Q_t = Q_1^{(3)} + 2Q_2^{(3)} + Q_3^{(3)}$$

$$\beta^{(3)} = \frac{2Q_2^{(3)} + Q_3^{(3)}}{Q_1^{(3)} + 2Q_2^{(3)} + Q_3^{(3)}}$$

$$\gamma^{(3)} = \frac{Q_3^{(3)}}{2Q_2^{(3)} + Q_3^{(3)}}$$

δ and higher order terms are identically zero.

For a group of four similar components, the MGL parameters are:

$$Q_t = Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}$$

$$\beta^{(4)} = \frac{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}{Q_1^{(4)} + 3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}$$

$$\gamma^{(4)} = \frac{3Q_3^{(4)} + Q_4^{(4)}}{3Q_2^{(4)} + 3Q_3^{(4)} + Q_4^{(4)}}$$

$$\delta^{(4)} = \frac{Q_4^{(4)}}{3Q_3^{(4)} + Q_4^{(4)}}$$

The following equations express the probability of multiple component failures due to common cause, Q_k , in terms of the MGL parameters for a three and four component common cause group are as follows:

Three component group:

$$Q_1 = (1-\beta)Q_t$$

$$Q_2 = \frac{1}{2}\,\beta\,(1-\gamma)Q_t$$

$$Q_3 = \gamma\,\beta\,Q_t$$

Four component group:

$$Q_1 = (1-\beta)Q_t$$

$$Q_2 = \frac{1}{3}\,\beta\,(1-\gamma)Q_t$$

$$Q_3 = \frac{1}{3}\,\beta\,(1-\delta)Q_t$$

$$Q_4 = \gamma\,\beta\,Q_t$$

➢ 3.4.4 Alpha – Factor Model [10]

Unlike the MGL parameters which are estimated from component failures, the Alpha factor parameters are estimated from system failure data. In the Alpha-factor model, failure rate per group depends only on size of group. This model enjoys low number of parameters, easy to estimate, but less obvious physical interpretation. The alpha factor model defines common cause failure probabilities from (1) a set of failure frequency ratios and (2) the total component failure frequency, Q_t . In terms of the basic event probabilities, the alpha factor parameters are defined as:

$$Q_k = \frac{k}{\left(\frac{m-1}{k-1}\right)}\,\frac{\alpha_k}{\alpha_t}\,Q_t \quad k = 1, \ldots m$$

$$\alpha_t = \sum_{k=1}^{m} k\,\alpha_k$$

For example, for a group of three similar components we have:

$$\alpha_1^{(3)} = \frac{3Q_1^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

$$\alpha_2^{(3)} = \frac{3Q_2^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

$$\alpha_3^{(3)} = \frac{Q_3^{(3)}}{3Q_1^{(3)} + 3Q_2^{(3)} + Q_3^{(3)}}$$

Note: $\alpha_1^{(3)} + \alpha_2^{(3)} + \alpha_3^{(3)} = 1$

The parameters of the Alpha-factor are related to MGL models as follows:

$$\alpha_1 = 3(1-\beta)$$

$$\alpha_2 = \frac{3}{2}\beta\,(1-\gamma)$$

$$\alpha_3 = \beta\gamma$$

Similarly,

$$\beta = \frac{2\alpha_2 + 3\alpha_3}{\alpha_1 + 2\alpha_2 + 3\alpha_3}$$

$$\gamma = \frac{3\alpha_3}{2\alpha_2 + 3}$$

Alpha factor model is considered to be non-conservative, non-causal, non transferable model; but the model is considered consistent with data.

➢ 3.4.5 Binomial Failure Rate (BFR) Model [10]

BFR is considered a statistical approach for quantifying CCFs. The underlying model is based on the multivariate exponential distribution developed by Marshall and Olkin[10]. For the quantification of CCF, it is assumed that common causes occur in accordance with a Poisson process. The BFR model considers two types of failures. The first (1) represents independent

component failures; the second (2) type is caused by shock (an event other than intrinsic, random or independent failures that occurs at a random point and acts on all the components in the system simultaneously) that can result in failure of any number of components in the system. According to BFR model, there are two types of shocks: lethal and nonlethal. When a **nonlethal shock** occurs, each component within the common cause component group (CCCG) is assumed to have a constant and independent probability of failure. The name of this model arises from the fact that, for a group of components, the distribution of the number of failed components resulting from each nonlethal shock occurrence follows a binomial distribution. The BFR model is, therefore, more restrictive because of these assumptions than all other multi-parameter models presented here. When originally presented and applied, the model only included this non lethal shock. Because of its structure, the model tended to underestimate the probabilities of failure of higher order groups of components in a highly redundant system; therefore, the concept of lethal shock was included. This version of the model is the one recommended. When a lethal shock occurs , all components are assumed to fail with a conditional probability of unity. Application of the BFR model with lethal shocks requires the use of the following set of parameters:

Q_I = independent failure frequency for each component.

M = frequency of occurrence of non lethal shocks.

P = conditional probability of failure of each component, given a non lethal shock.

Ω = frequency of occurrence of lethal shocks.

The BFR model is considered less conservative than the Beta-factor model for higher redundancy levels as well as more restrictive than all other multi-parameters models. BFR is generally considered non-conservative, causal, transferable, and non consistent with data.

One of the advantages for this model is (1) much information can be extracted from scarce data, and (2) distinction can be made between partial and total failures. On the other hand, BFR model main disadvantages lies in (1) being a complicated estimation process, and (2) CCF causes are assumed to have equal severity.

3.5 Summary of Parametric Models [14]

Estimation Approach			Model	Model Parameters	General form for multiple component failure frequency
NONSHOCK MODELS	Direct		Basic Parameter	$Q_1, Q_2, \ldots Q_m$	$Q_k = Q_k$ k=1,2,.....m
	INDIRECT	Single Parameter	Beta Factor	Q_t, β	$Q_k = (1-\beta)*Q_t$ k=I $Q_k = 0$ $2 \leq k < m$ $Q_k = \beta * Q_t$ k=m
		Multi-Parameter	Multiple Greek Letter	$Q_t, \beta, \Upsilon, \delta$	$Q_k = \frac{1}{\binom{m-1}{k-1}} \binom{k}{i=1} \pi \; p_i (1-p_{k+1}) Q_t$ $p_1 = 1, p_2 = \beta, p_3 = \gamma \ldots, p_{m+1} = 0$
			Alpha Factor	$Q_t, \alpha_1, \alpha_2, \ldots \alpha_m$	$Q_k = \frac{k}{\binom{m-1}{k-1}} \frac{\alpha_k}{\alpha_t} Q_t \quad k = 1, \ldots m$ $\alpha_t = \sum_{k=1}^{m} k \, \alpha_k$
SHOCK MODELS			Binomial Failure Rate	Q_t, μ, ρ, ω	$Q_k = \begin{cases} Q_1 + \rho(1-\rho)^{m-1} & k=1 \\ \mu\rho^k (1-\rho)^{m-k} & k \neq 1, m \\ \mu\rho^m + \omega & k=m \end{cases}$ $Q_t = \sum_{k=l}^{m} \binom{m-l}{k-l} Q_k^{(m)}$ $\sum_{k=l}^{m} \binom{m-l}{k-l} = \frac{(m-l)!}{(m-k)!(k-l)!}$

Table 3.1 Parametric Models

3.6 Issues with CCF Models

The CCF models used in PRA were not developed with event and condition assessment in mind. As a result, many issues arise with PRA models in their application to failure event and condition assessment, such as:

➢ 3.6.1 CCF Models are not Causal

The Beta factor and the alpha-factor models do not incorporate causes of failure explicitly. The parameters in the PRA models are estimated from a combination of past failure events, which had a variety of causes. The unknown parameter *p* (failure probability) used in these models is a lumped parameter which encompasses all possible causes of failure. Thus, the CCF parameter values are not specific to a single cause, such as poor maintenance practices or over heating in the system.

➢ 3.6.2 BPM Models Employs Symmetry Assumption

Most CCF models apply a simplifying assumption that each component in a CCCG has the same total failure rate or failure probability, denoted by λ_t and Q_t, respectively. If only one component in a CCCG is degraded, and thus has a different λ_t or Q_t than the other components in the CCCG, the symmetry assumption breaks down.

3.6.3 CCF is not Modeled Across Component or System Boundaries

Most PRA models incorporate CCF only within the CCCG boundaries, meaning that a CCCG does not include components of a different type in the same system, or components from more than one system. This is fundamentally a limitation of the available CCF database, which is too sparsely populated to allow estimation of CCF parameters outside the CCCG boundaries. Causes of failure are of course not limited by such boundaries. This makes the risk estimates approximate and potentially non-conservative.

3.6.4 Impact on More than One Failure Mode not Captured

The current consensus CCF model is also tied to specific component failure modes (e.g., failure to start). A performance deficiency, such as poor maintenance or poor quality control, which results in a failure to start of a component in a CCCG, could also impact the CCF probability of multiple components in the CCCG failing to run as well. However, such an impact on an unobserved failure mode cannot be captured in the current parametric CCF models.

3.6.5 Estimates of Alpha Factors are not Plant-Specific

The alpha-factor estimates in the CCF Parameter Estimation Update, which are used to calculate CCF probabilities models, are generic for a type of component. Because they are not plant-specific, they contribute to the approximate nature of Event & Condition Assessment risk estimates.

3.7 Summary

This chapter introduced the parametric models briefly including its respective advantages and disadvantages. Also, it was emphasised how Common Cause Failures (CCF) are significant when evaluating component's or system's failure and when conducting Probabilistic Risk Analysis (PRA) analyses. The importance of CCF in Nuclear Power Plant (NPP) operation, reliability and safety is evident through the mandatory PRA and PSA studies conducted in each NPP site periodically for licensing. Furthermore, the International Atomic Energy Agency (IAEA) has issued numerous standards for the member states to adhere to - in an effort to avoid and limit the potential catastrophic effect of CCF such as External Events . The next chapter will discuss critical components and functional areas affected by severe accidents in NPPs and potential mitigating consequences.

Chapter 4

Mitigating Consequences of Severe Accidents in NPP

4.1 Introduction

The 2011 accident at the Fukushima Daiichi NPP caused a major ripple effect in the nuclear community on how they should view safety and how to address severe accident management and onsite recovery. One of the primary lessons learned from the accident at Fukushima Daiichi NPP was the challenge presented by a loss of safety-related systems following the occurrence of a beyond-design-basis external event. Further, the extended loss of alternating current (AC) power due to a tsunami event lead to the loss of core cooling and a significant challenge to containment which lead to explosion of the containment building causing contamination of the site and its surrounding with radioactive (spent) fuel material which cause a major evacuation of the nearby community. Since the accident, many emergency preparedness and response plans are being developed to cope with nuclear or radiological emergency scenarios ranging from small spillage of radioactive material to a major nuclear accident releasing large-scale radioactivity like Fukushima above. Many (IAEA) member states developed programs to manage severe accidents scenarios such as: implementing emergency operating procedures, conduct abnormal operating procedures, pre-planned alarm response procedures, setting up Severe Accident Management Guidelines (SAMG), and extensive damage mitigation guidelines. Also, the Fukushima accident demonstrated the need for effective post-accident management, including radiological evaluation, efficient mechanisms

for decision making, control and management of contaminated goods, resettlement and much more.

4.2 Defense in Depth Strategy for External Events and Severe Accidents:

The lessons from Fukushima and other severe accidents shine the light on the importance of strengthening reactor defence in depth strategy and how it should minimize and manage severe accidents and external events. NPPs design capabilities in beyond-design-basis accident conditions should include [16]:

a) Response of the main systems and components' "overpressure"

b) Containment protection and prevention of unfiltered releases of radioactive products

c) Control capabilities for hydrogen and other combustible gases (i.e. igniters, PARs)

d) Make-up capabilities for the steam generators, primary heat transport system and connected systems, moderator, shield tank, and spent fuel bays

e) Design requirements for the self-sufficiency of a plant site such as availability and survivability of equipment and instrumentation following a sustained loss of power and capacity to remove heat from a reactor core

f) Control facilities for personnel involved in management of the accident

g) Emergency mitigating equipment and resources that could be stored offsite and brought onsite if needed

An effective response to an emergency requires strong linkages between accident management and emergency preparedness. Accident management in NPPs must be able to respond to any credible accident in order to [17]:

- Prevent the escalation of the accident
- Mitigate the consequences of the accident
- Achieve a long-term safe stable state after the accident

To achieve the above goals, a thorough mitigation plant that comprises a cohesive set of plans and arrangements undertaken to ensure that, if an accident occurs:

- The safety systems and the available structures, systems and components (SSCs) can be used to control the reactivity, cool the fuel and contain the radioactive materials such that damage to the reactor and harm to workers, public, and environment is prevented or mitigated
- Trained personnel with responsibilities for accident management are adequately prepared to utilize available resources and procedures to perform effective accident management actions

During a nuclear emergency, the practical goals of emergency response are:

- Regain control of the situation
- Prevent or mitigate consequences at the scene
- Prevent the occurrence of deterministic health effects in workers and the public

NPPs should be designed and maintained to deal with all possible external events and severe accidents effectively. There are numerous and complex systems in NPPs and each have its risk factor contributor to the overall safety of the plant. Next, we will discuss the importance of each system and failure consequences to NPP.

4.3 Managing Main Systems in NPP during External Events

Typical nuclear power plant site consists of many complex systems to operate and maintain the reactor core functional and in a safe manner to the public and surrounding environment. However, loss of any of these systems may have a devastating effect on the operability and safety of the NPP. Below are samples of how NPPs are affected by the loss of main systems post EE or severe accidents:

➢ 4.3.1 Effects of loss of Onsite (AC) Electric Power:

The availability of AC power is essential for the safe operation and accident recovery in all NPPs. If a plant experiences a loss of offsite power (LOOP), emergency diesel generators (EDGs) will provide onsite AC power. However, if the EDGs were rendered unavailable or fail to provide AC power to the plant, then the plant will experience complete station blackout (SBO). The loss of AC power will have a significant impact on an NPP's ability to achieve and maintain safe shutdown conditions. In fact, loss of AC power is a significant contributor to the risk associated with plant operation, contributing more than 70 percent of the overall risk at some plants [15]. Further, achieving safe reactor shutdown in the event of Loss of Onsite Power (LOOP), the plant must rely on components that do not require AC power, such as turbine or diesel driven pumps. Thus, the reliability of such components, the capacity of direct current (DC) batteries, and the timeliness of offsite power restoration are important contributors to SBO risk. Addressing SBO risk issue, some countries issued regulations to combat such a scenario. In the United States, the NRC issued the SBO rule (10 CFR 50.63) which requires NPPs to have capability to withstand SBO and maintain core cooling for a minimum duration ranging 2-16 hours. Further, NPPs also

were required to enhance procedures and training for restoring offsite and onsite AC power sources as well as implement necessary modifications to NPPs, such as adding more sources of emergency AC power, to restore power to the site.

➢ 4.3.2 Onsite and Offsite Communications

Effective communications is integral to handling emergencies and post management of severe accidents. Managing an external event effectively requires communication between the site's command centre unit and the onsite crew to execute EOPs & AOPs as well as be in touch with the offsite emergency and technical response teams to time manage resources, personnel and emergency equipment suitable to the event. In the event of a severe nuclear accident it is important to provide a way to power communications equipment needed to communicate onsite (e.g., radios for response teams and communication between facilities) and offsite (e.g., cellular telephones, satellite telephones) during a prolonged SBO. Establishing communications on site post a severe accident or external event should be a top priority when establishing a mitigation strategy.

➢ 4.3.3 Accident Management:

Possible accident scenarios must be identified before the start of a plant's operation. For each identified accident, a structured procedure must be developed along with its Emergency Operating Procedures (EOPs) and severe accident safety guidelines (SAMG). Although the accident scenarios are limitless, the objective of managing severe accident is not. The main priority in any severe accident or post external event is to restore and maintain UHS, cooling of the spent fuel pool and maintain the integrity of the containment structure. Also, accident

management must be able to time manage all resources effectively and in a timely manner such as skilled personnel and emergency equipment. Further, thorough pre-planning is key to successfully contain an accident. Evaluating site's emergency preparedness is required and frequent audits are needed to continually be in "standby" in the face of any potential emergency or event.

➢ 4.3.4 Radiation Protection and Pre-Staging of Potassium Iodide

In an effort to protect public health and ensure community safety from the inadvertent release of radioactive materials, a defense-in-depth strategy for NPPs should include multiple layers of radiation protection such as (1) proven safe design, construction and operation (2) pre-planned and pre-staged mitigation processes and features to prevent radioactive releases and (3) emergency preparedness programs that include measures such as sheltering and evacuation and distribution of Potassium Iodide. Further, the defense-in-depth strategy for NPPs should also encompass multiple physical barriers to contain and limit the radioactive release in the event of an accident such as: fuel cladding, the reactor coolant pressure boundary, and the containment [18]. Radiation protection and public safety need to be maintained at all times before and after an external event or severe accident. Loosing public confidence and support to nuclear energy would be an uphill battle to regain. Thus, constant feed of information to the public should be maintained during managing an emergency event and that includes the amount of and type of material radiation release to the public. Second, in the event of major and/or extended radiation release into the surrounding community, the potassium iodine (KI) distribution zone should be adequate and accessible to the public. Also, all levels of

government must have plans to combat radiation release as part of their site approval, and health and emergency procedure policies.

4.3.5 General Safety Features in NPPs

Part of mitigating consequences of external events and severe accidents is that the NPPs should feature built-in safety measures to reduce the impact of an accident such as having biological shields, various effective safety systems and interlocks; this in combination with periodic safety audits combined with operations and administrative safety procedures should mitigate and minimize the consequences of nuclear accidents. Also, the reactor main components and systems should have auxiliary access points well protected and at different locations and elevations in order to connect emergency portable systems and/or re-direct coolant to avoid major core melt down, loss of UHS or cooling of spent fuel pool. Also, the NPP should feature reliable measuring devices and sensors to continually send information on the status of the containment structure, reactor core and SG in effective planning and management of the accident and event. Some engineered safety features in NPPs to mitigate the consequences of a severe accident and/or external event are [19]:

- Vapour Suppression System to limit the peak pressure of containment during a loss of coolant accident condition
- Liquid Poison Injection System for long term sub-criticality of reactors
- Reactor Building Coolers to bring down the primary containment pressure during an accident condition

- Secondary Containment Recirculation System to reduce activity release, using multi-pass filtering by recirculation

4.3.6 Effects of Loss of Ventilation

Loss of ventilation is typically due to a SBO event. Equipments within the containment structures suffered from loss from ventilation is beyond the scope of this paper since usually it is enveloped by the loss of coolant accident (LOCA) safety risk analysis. Loss of ventilation to equipment located outside the containment structures that are considered dominant areas of concern are:

- HPCI/HPCS and RCIC rooms - decay heat removal equipment (BWR Reactors only)
- Steam driven AFW pump room - decay heat removal equipment (PWR Reactors only)
- Main stream tunnel (BWR only) - high temperature cut out for decay heat removal equipment

In addition, loss of ventilation to the site is an added safety risk since sensitive areas depend on ventilation for continued operation such as the "control room". The restoration of the ventilation system post severe accident or an external event should be immediate after the event hits. Adequate emergency planning and auxiliary ventilation systems should be readily available for deployment and operation to supply ventilation to site.

4.3.7 Containment

Containment systems vary in design between different types of reactor. In CANDU reactors, for instance, the containment design involves the use of a negative-pressure (vacuum building) concept to prevent an uncontrolled release. Over time the vacuum will depletes due to air

leakage. For planning purposes, the sequence of events and hold-up times to be used in the case of the CANDU reactors are generally as follows [20] :

a. Containment isolation (or "box up") is engaged after a short interval after a loss-of-coolant accident (LOCA). During this short interval, potential initial release of radioactivity material (known as a “puff” release) may occur
b. The interval between any initial puff and the start of a sustained emission could be as short as about one hour (impaired containment) but can be contained for a minimum of 2 days (Pickering plant), 2½ days (Bruce plant), or 7 days (Darlington plant)
c. The duration of an emission (whether sustained or intermittent) could be several weeks. The largest release of radioactivity would most likely occur during the first few days

In NPPs the operation of containment isolation valves either fail in the safe condition in accordance with the design bases of the plant or can be manually closed. Further, the UHS system is built according to defence in depth strategy, where a combination of redundant locked closed and automatic isolation valves for reactor coolant pressure boundaries and any containment penetration line directly connected to the containment atmosphere must be in place. Isolation valves can operate automatically, manually or via remote manual access operation. Most containment isolation valves are in the normally closed or failed closed position during power operation. Typically, these valves are air-operated and failed closed valves (no need for AC power to close). In the event where coolant is lost, access to a vast body of water reservoir is required and the necessary equipment to maintain circulation of the water to stabilize reactor core temperature.

4.3.8 Containment venting

In the event of a loss of core cooling, the coolant and moderator will eventually boil which may lead to potential formation of gases such as explosive Hydrogen gas which could explode in a presence of a spark causing a significant damage to the containment structure. Therefore, NPPs must have a means to vent the containment in order to maintain the structural integrity of the containment. Systems such as emergency containment filtered ventilation (ECFV) can readily be installed, as a safety feature in NPPs, to vent the containment. ECFV system will protect the containment envelope if the internal containment pressure approaches the containment strength limit and to remove radioactive materials from any gases vented from the containment in a severe accident. ECFV uses a high-efficiency scrubber and filtration unit to filter out the vast majority of fission products so radiation exposure to the public would be limited to acceptable levels in the event of a release [16].

4.3.9 Active/Passive Safety Systems for Core Decay Heat Removal

Loss of site AC power would cause the "active" UHS to be offline due to loss of power to pumps. In the aftermath of an external event or severe accident causing SBO, it is important that decay heat generated from the reactor core and heat from irradiated spent fuel be removed and controlled. Loss of cooling of the irradiated fuel bays is generally a lesser concern than loss of core cooling as much more time is available before the fuel overheats. However, irradiated fuel bays generally have fewer alternative cooling options than the core; therefore the issue is still important. Advanced reactor designs have incorporated several "passive" systems to address

removal decay heat in reactor core, steam generator and spent fuel pool. Some of the "passive" heat sink systems are:

- Pre-pressurized core flooding tanks (accumulators)
- Elevated tank natural circulation loops (core make-up tanks)
- Gravity drain tanks
- Passively cooled steam generator natural circulation
- Passive residual heat removal heat exchangers
- Passively cooled core isolation condensers
- Sump natural circulation
- Containment pressure suppression pools
- Containment passive heat removal/pressure suppression systems
- Passive containment spray First step in managing post severe accidents and/or an external event would require the restoration of AC power to the "active" UHS (i.e. pumps). If failed, then maintaining large water volume to "passive" cooling systems would be a priority to safely control reactor core temperature and avoid fuel failure, core damage and/or radioactive release due to containment failure. A mitigation plan must be readied for such an event including planning of required portable equipment, adequate and strategic storage (for deployment) of these equipment and adding auxiliary connection points to access "active" and "passive" UHS systems.

➢ 4.3.10 Hydrogen management

In any light-water nuclear power reactor, hydrogen is formed by radiolysis decomposition of water. Hydrogen gas formation in the containment structure following a severe accident presents a significant challenge in NPPs safety. Hydrogen risk mitigation measures are [16]:

- Pre-inertization with nitrogen in most of the BWR containments,
- Passive autocatalytic re-combiners in large dry PWR containments,
- Igniters for PWR ice condenser and BWR Mark III containments.

❖ 4.3.10.1 Inertization of Containment Atmosphere in NPPs:

Pre-inertization: This process is specific to BWR plants due to its relatively small containment. Cold stored nitrogen (after being heated by an air heated vaporizes) is fed into the containment by using the existing ventilation system during normal operation. Thus reducing oxygen in the containment (<5%) will lead the risk of hydrogen combustion to near zero.

- Post-inertization: Post accident inertization process is specific to PWR (large) containment NPPs which involves injection of non-combustible or combustion-inhibiting gases such as Carbon dioxide and Nitrogen gases into the containment atmosphere. Complete inerting (i.e. combustion suppression at all hydrogen concentrations) is possible only when the carbon dioxide or steam concentration exceeds approximately 60% by volume concentration in air; further, inerting with nitrogen requires in excess of 75% by volume concentration

❖ 4.3.10.2 Hydrogen Igniters Types in NPPs

- Glow plug igniters: are electrical resistance heaters that produce a surface temperature of 800 to 900°C, which is a positive ignition source for flammable mixtures of hydrogen air steam. They require a separate power source due to the high power requirement (150 to 200W each)
- Spark igniters: hydrogen gas have the lowest spark ignition energy of any combustible fuel. Spark igniters require small power thus they are well suited to battery power
- Catalytic igniters: Catalytic igniters employ the heat of $H_2 - O_2$ reactions at a spatial catalytic element to produce surface ignition temperatures high enough to cause ignition. Catalytic igniters are self-actuating, self powered and continuously available
- Spontaneous ignition: a small spark produced by any electrical or mechanical equipment is enough to ignite a hydrogen air mixture. Hot surfaces also can serve as igniters as well as static electricity
- Catalytic recombination: Catalytic re-combiners use catalysts to oxidize (recombine) the hydrogen and are operable outside the limits of flammability. PARs do not need external power or operator action

➢ 4.3.11 Coolant

Loss of coolant post severe accident or external event add a significant risk to safety of NPPs. Thus, coolant make-up provisions such as various auxiliary water connections and dedicated lines intended to replenish water inventory in important plant systems are an important line of defence against accidents progressing to severe core damage. Coolant in NPPs is required to a

variety of systems to prevent, slow down or terminate the core fuel degradation process. These systems include: SG, calandria, shield tank, calandria vault and the spent fuel bay. Water is typically provided either by in-containment reserves (such as a dousing tank) or by an external connection to the reactor building.

➢ 4.3.12 Irradiated fuel bays

Fuel bays contain significant quantities of irradiated fuel. Because of decay, fission product inventories in the spent fuel decrease over time. Nevertheless, the long-lived radioactive materials could pose a significant threat if the spent fuel is uncovered and subsequently overheats. The decay heat from an irradiated fuel bay is not significant compared to the reactor core, but spent fuel pools have limited cooling resources compared to reactor core. Thus, provision must be made to restore cooling and heat removal to spent fuel bay post severe accident. Portable pumps, cooling equipment and access to large body of water are part of defence in depth to manage heat decay of irradiated fuel bays.

4.4 Mitigation: Emergency Equipment

➢ 4.4.1 Equipment Protection / Storage:

Emergency equipment storage is a detrimental step to the mitigating consequences of external events and severe accidents. Failure to provide adequate and safe storage to the emergency equipment will render the equipment unavailable or un-accessible as well as will add further safety risk to the site. Hence, emergency equipment should be stored be adequately protected and secured in order to ensure emergency equipment availability and should be functional and

reliable when needed. Emergency equipment storage structure should adhere to IAEA standards on storage for each EE type (see chapter 2), including seismic event, as per site's DBEE as well as according to regulations of the member state, if any (i.e. in case of flood, emergency equipment should be protected either by barriers or elevation)

➢ 4.4.2 Emergency Equipment Deployment plan:

Emergency equipment deployment should be evaluated and studied for each EE and severe accident situation in order to manage post accident situation adequately and swiftly. Accessing emergency equipment in a timely manner when needed is an important task during management of post severe accident or external event. Below are some considerations for the deployment of emergency equipment following an External Event:

- If reasonable warning time is given prior to an external event (such as freezing rain storm), the plant most likely is being shut down. In this case, emergency equipment could be tested and readied (i.e. connecting portable pumps for use prior to the arrival of the critical flood level)
- Site Accessibility: moving equipment from storage to the required location on site for deployment, the accessible road should be reviewed for potential soil liquefaction that could impede movement following a severe event. Use/access to emergency heavy mobile equipment at NPP site immediately after EE should be part of the mitigating consequences plan
- Plant design should accommodate for auxiliary connection point for Emergency Equipment to be deployed and/or operate such as: electric power, water supply,

ventilation equipment, UHS. This includes both the connection point and any areas that plant operators will have to access to deploy or control the capability

- A secondary reliable water supply is integral to the mitigating consequences of severe accidents. Thus contingency plans should be in place to source and secure water supply during accidents. Also, special equipments (i.e. portable pumps, hoses) are needed and must be part of the Emergency Equipment plan
- If power is required to move or deploy the Emergency Equipment (such as to open the door from a storage location), then power supplies (i.e. portable generators, cables and batteries) should be provided as part of the Emergency Equipment deployment plan
- A means to move emergency equipment should be provided that is also reasonably protected from the event. Site roads blockage and Infrastructure damage to in and around the NPP site could be an immediate result from the event. Therefore EE plan should secure EE

4.4.3 Synchronization: Off-site Resources with On-site Demands

For effective management of any external event or severe accident requires Central Command Centre (CCC) to coordinate and synchronize emergency equipment between off-site storage and onsite in a timely and effective manner. CCC will administer and manage emergency equipment as pre-approved and pre-planned AOPs, EOPs and safety guidelines as see fit for each event.

4.5 EME *for* Extreme Wind Event [21]:

Extreme Winds present a challenge to both on-site and off-site resources to protect against such event. Typically, the damage from tornadoes is relatively localized whereas hurricanes damage is widespread and causes a greater damage to local infrastructure and the surrounding site (such as flooding & downing trees) which is needed to be considered in the planning process and mitigation against hurricanes. The characterization of hurricanes includes the fact that noticeable time is available to the NPP site to prepare against the impact of severe hurricane. This early warning notice of hurricane arrival is an advantageous feature that allows the pre-planned mitigation process and equipment for early deployment in extreme wind storms /hurricane. The pre-staging and advanced deployment of mitigation equipment in the event of tornadoes is less effective than in hurricane event. However, the impact of tornadoes on the local infrastructure is much more limited than hurricanes, just debris dispersal. Therefore, protection and deployment of emergency equipment during extreme wind should follow these recommendations:

➢ 4.5.1 Equipment Protection/Storage

- Emergency Equipment should be stored adequately protected and secured in order to ensure Emergency equipment availability and reliability when needed. Emergency Equipment storage structure should adhere to IAEA standards on storage for an extreme wind event (see chapter 2) as per site's DBEE as well as according to regulations of the member state, if any.

- Storage site should be protected from tornado missiles and hurricane missiles in order to allow reliable and safe deployment of emergency equipment. Consideration should be given to storage in robust location and in lower levels of the building to minimize the probability of damage caused by wind missiles.
- Storage of mitigating emergency equipment should take in consideration the path tornadoes take. In general, tornadoes travel from the West or West Southwesterly direction; thus, equipment storage should be likely in the direction of the North-South arrangement, where possible.
- Stored mitigation equipment in extreme wind storms should be secure and fastened adequately.
- Storage locations of emergency equipment should be separated by distance so that extreme winds do not destroy all locations.

4.5.2 Deployment of Emergency Equipment

Considerations for deploying emergency equipment during an extreme wind event are:

- Since early warning of hurricanes and tornadoes are given to NPP site, emergency equipment such as diesel generators and portable pumps should be connected in advance of the event tested and readied.
- Extreme Wind event may force the ultimate heat sink offline due to debris and storm surge considerations.
- Since extreme wind may cause significant debris in the NPP site, therefore consideration to clear the blocked roads from debris and create access routes to emergency

equipment deployment must be evaluated and considered in the pre-planning and staging process of the event.

- A reliable and safe means of transportation to move emergency equipment should be considered in the pre-planning and staging process of the event.
- The ability to move equipment and restock supplies may be affected during extreme wind storm and consideration should be taken to overcome this in order to plan for deployment of emergency equipment.

4.6 EME *for* Snow, Ice and Extreme Cold Temperature Event [21]:

Extreme low temperature, snow and freezing storms, or a combination of any, present challenges to NPPs and potential damage from these events to the site is dependent on the site layout, plant design, and regional weather hazards present. From a plant design prospective, snow is considered when evaluating the site's building roof loadings; similarly, ice and extreme cold temperatures are considered when evaluating potential impacts on the intake structure and safety related equipment. This general category of snow, ice and extreme low temperatures includes the following hazards:

• Avalanche

• Frost

• Ice cover

• Frazil ice

• Snow

• Extreme low temperatures

Snow and ice storms and extreme low temperatures may cause damage to both on-site power grid and off-site power capabilities (such as intake structures). Loss of AC power and EDGs may lead to or be a major contributor to UHS. Also, storms could impact the movement and deployment of emergency and portable equipment and resources both on-site and off-site. Therefore, protection and deployment of emergency equipment during snow and storms or extreme low temperature should follow these recommendations:

4.6.1 Equipment Protection/Storage

NPP site may potentially experience extreme low temperature; as a result the emergency equipment stored and procured on-site or off-site should be suitable for use during the anticipated range of low temperature as well as in snow/ice storm conditions. The following are considerations to protect emergency equipment from snow, ice, and extreme cold hazards:

- Due to potential heavy snow/freezing storms, emergency equipment should be stored according to the following:

  a) Storage structure should meet IAEA's standards as per chapter 2. Also, storage structure should meet the plant's design basis for the snow, ice and cold conditions (e.g., existing safety - related structure).

  2) Storage structure should conform to site's design basis for snow, ice and extreme low temperature.

- Access to stored emergency equipment should be in a timely manner by having accessible roads to transport them. The equipment should also be maintained at a temperature within a range to ensure its functionality when needed. For example,

storage should be a heated enclosure or should be accessed by direct heating (e.g., jacket water, battery, engine block heater, etc.).

4.6.2 Deployment of Emergency Equipment

Consideration that apply to the deployment of emergency equipment for snow, ice, and extreme low temperature hazards:

- Emergency equipment should be stored to function in the extreme conditions applicable to the site. Also, safety for the workers should be evaluated when performing AOPs and EOPs by plant personnel.
- Sites exposed to extreme snowfall and ice storms, accessible roads and emergency routes should always be available; thus, snow/ice removal is required as needed to obtain and transport emergency equipment from storage to its location for deployment.
- Potentially, snow and freezing storms and extreme temperature the UHS and flow path may be affected due to ice blockage or formation of frazil ice. Consequently, this may affect the performance of emergency equipment when called upon. For example, if UHS water is to be used as a makeup source, some additional measures may need to be taken to assure that the emergency equipment can utilize the water.

4.7 EME *for* External Fire [21]:

➢ 4.7.1 Equipment Protection/Storage

Protection of EME equipment storage area against seismic event can be done through:

- Having storage structure design that meets DBEE for seismic event. Selection of structure material storage location and construction should adhere to ASCE 7-10 seismic specification, *Minimum Design Loads for Buildings and Other Structures*.
- Having storage structure evaluated and protected from seismic interactions to ensure that unsecured and/or non-seismic components do not damage the EME.

➢ 4.7.2 Deployment of Emergency Equipment

Considerations that should take place for the deployment of EME in a Seismic event are:

- Review of all potential EME deployment access roads; attention should be made to possible road obstacles (i.e. high water level or potential soil liquefaction) that could impede movement of EME or deployment following a severe seismic event.
- Multiple connection points (separated by distance, elevation and location) for EME is required to access the NPP.
- Additional secondary EME might be required to provide power to access main EME storage, or provide water supply (i.e. from underwater berm) to the NPP.

  Protection of deployment trucks or machinery from Seismic event is required in order to move EME to required location.

4.8 EME *for* External Flood [21]:

➢ 4.8.1 Equipment Protection/Storage

Considerations for the deployment of EME in an External Flood hazards are:

- The equipment should be stored above the flood elevation and in a structure designed to protect the equipment from the flood.
- Storage areas that are potentially impacted by a rapid rise of water should be avoided.

➢ 4.8.2 Deployment of Emergency Equipment

Considerations which apply to the deployment of EME for external flood hazards are:

- If warning time is given, plant configuration could be established to optimize EME deployment.
- Ensure ample supplies, protective equipment and spare parts are stocked and accessible during external flood to support successful long-term EME deployment.
- EME equipment should be designed and deployed to support alternative or supply to heat sink, in the event of UHS.
- Consideration to protect or provide alternate sources of fuel oil to continue powering EME in flood conditions.
- Connection points for portable equipment should be reviewed to ensure that they remain viable for the flooded condition. Also, consideration to provide water extraction pumps and hoses is required for deployment of EME strategies.
- Considered means (trucks, bulldozers, boats) to move EME equipment should be provided as well as they should be reasonably protected from the event.

4.9 Summary

The chapter presented critical components and functional areas in NPPs that could potentially be affected by severe accidents that may develop as a consequence of Beyond Design Basis Events (BDBEs) such as those initiated by extreme external events. A Practical and accurate assessment of NPP emergency readiness and overall NPP vulnerability is pressing. Next chapter will present Emergency Mitigating Preparedness (*EMP*) model capable of providing NPPs the tool to gauge its mitigation readiness based on four criteria: emergency mitigating equipments, inherent safety features/systems in the NPP, human factor and physical barriers.

Chapter 5

Modeling and Assessment of

Emergency Mitigating Preparedness in NPP

5.1 Introduction

Nuclear Power Plants (NPPs) are vulnerable to the powerful impact of External Events (EEs) such as major flooding, massive external fire, extreme low temperature/snow storm, powerful wind and Tsunami. The recent Fukushima accident in 2011 proved the impact of EEs are devastating to the nuclear site's structure, plant personnel's health and safety, neighbouring community's well being - safety - life style - future development, and finally the negative impact on the environment and economy which is incalculable. In fact the massive site reconstruction and community rebuilding efforts in addition to the land and sea radioactive material cleanup is projected to be extremely expensive and long term projects to take on. The current safety evaluations of NPPs that are based on either deterministic or probabilistic methods are not sufficient to protect against EEs. Most of the current approaches are (1) subjective (2) require expert advice (3) do not reflect redundant defense strategies and (4) do not factor in human error and/or lack of corporate safety culture to name a few. As a result, a more objective and practical evaluation model is required to give NPP the tool for adequate emergency mitigation planning against BDBE or EEs and to provide an accurate ***NPP Vulnerability*** indicator gauge to allow NPPs to improve in areas of planning, site design, worker readiness to execute effective mitigation plans and finally to foster a culture of safety to protect personnel, the community and environment.

The **E**mergency **M**itigation **P**reparedness (EMP) assessment model is proposed as an inclusive and practical approach to primarily ***quantify emergency mitigation readiness*** as well as ***NPP Vulnerability*** due to EEs. The proposed *EMP* model and assessment encompasses EE *relative risk ranking* , site design, human factor and plant readiness. The model is objective in approach and practical to execute. The assessment process identify potential risk gaps or opportunities to protect site structures, manage and maintain reactor core integrity, control and contain spent fuel and prevent radiation spread, manage various emergency scenarios safely and effectively and provide greater protection to personnel, the public and environment. *EMP* model is not dependent on expert advice and account for in-depth defence strategies, human factor and other site design features. *EMP* provides a thorough and comprehensive mitigation plan based on four pillars: (1) emergency equipment, (2) inherent plant safety systems, (3) NPP physical barriers and (4) human factor. In the event of the aftermath of BDBE or EEs, the *EMP* assessment model will position the nuclear site to mitigate potential severe accidents effectively. Proper application of the *EMP* model will enable the NPP to effectively provide better control and containment of the reactor core and other major components (SGs & Turbines). The main pillars evaluation is systematic (as will be discussed in later sections) and is directly dependent on EE risk. The assessment model requires quantifying the Alpha factors (which will be discussed later). The alpha factors (not to be confused with the alpha factor from the Alpha-Model discussed in chapter 3) are relative safety indices which are specific to individual NPP. Evaluating each factor is done through a series of three steps: the (1) first step is to complete the listing of required equipment, procedures and systems needed to address specific EE, (2) second step is to produce detailed features and characteristics needed and

required of the first criterion step (layer) and finally (3) third step expresses the test parameters required to evaluate the second layer's component, system or procedure. Combined with Relative risk ranking of EE for a particular NPP, the assessment model will provide an EMP emergency mitigation preparedness value which potentially provide NPP Vulnerability value as per the model's assumptions.

5.2 EMP Assessment model

▪ 5.2.1 Mathematical Model: Expression

As discussed earlier, the EMP is a function of emergency mitigation readiness for NPP through: EME, Human Reliability, Safety Features and Physical Barriers, such as:

$$EMP = f(\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2}, \boldsymbol{\alpha_3}, \boldsymbol{\alpha_4})$$

The EMP assessment model, in summary, is described in mathematical terms as follows:

$$\textbf{EMP} = \sum_e \boldsymbol{P_e}\left[\frac{\mathbf{1}}{\mathbf{4}}\left(\boldsymbol{\alpha_1} + \boldsymbol{\alpha_2} + \boldsymbol{\alpha_3} + \boldsymbol{\alpha_4}\right)_e\right] \quad | \quad \mathbf{0} \leq \boldsymbol{EMP} \leq \mathbf{1} \qquad (5.1)$$

Where:

e = represents a specific External Event to the NPP site (i.e. Fire, Flood, Wind,Tsunami)

P_e= Relative Risk Ranking (for Specific EE)

α_1= Emergency Equipment Factor (safety index for Specific EE)

α_2= NPP Inherent Safety Features factor (safety index for Specific EE)

α_3= Human Factor (safety index for Specific EE)

α_4= NPP Physical Barriers factor (safety index for Specific EE)

***NPP Vulnerability* of a NPP due to EE can be estimated to be:**

***NPP Vulnerability* = 1 - EMP** (5.2)

EMP Model Assumptions:

- All EMP Alpha factors are considered independent of each other and has equal weight. The assumption of no shared dependency between the four factors is supported and evident through the evaluation process and test criteria (discussed later) for each alpha factor. Equal weight assumption is based on all factors are essential to the success of mitigation preparedness plan equally. A weakness in the any alpha factor will render the emergency readiness potential failure.
- **NPP Vulnerability** (or potential failure to protect or to prevent hazard from occurring) term is assumed to be the complement of emergency mitigation preparedness (or potential success). This assumption is similar to evaluating (equipment) reliability for being the complement of (equipment) failure.
- ***Relative Risk Ranking*** evaluation is a based on the NPP's site EE statistical, ecological and historical data.

The *EMP* assessment model includes four main alpha-factors to quantify ***NPP Vulnerability:*** (1) emergency equipment capability (2) inherent NPP safety features and systems (3) available NPP physical barriers and finally (4) human factor. The evaluation of the ***NPP Vulnerability*** can be quantified directly by evaluating the effectiveness of the mitigation plan designed for the nuclear site. The *EMP* assessment model thoroughly and analytically evaluates a mitigation preparedness plan of a NPP based on examining the four alpha-factors. The model accounts for the importance of potential EE faced by the NPP as defined in the site's initial DBEE. Relative risk ranking method is executed to evaluate EE potential to the site which if found critical in

quantifying *EMP*. Further, the assessment model employs alpha-factors to evaluate each main area of the mitigation plan. The current presentation of the *EMP* model implies that the four alpha-factors are of equal weights and independent of each other. We will discuss later the "Relative risk ranking" and "alpha-factors" and their importance in equation (5.1).

5.2.2 **Relative Risk Ranking: P_e**

The ***EMP*** assessment model demonstrates the importance of each EE that could potentially be faced by the NPP. Based on initial DBEE report for NPP, the EE are assigned a potential risk probability. Relative risk ranking is a method where EE are tested among each other to reflect respective relative risk ranking (ratio) that is used in the *EMP* model. To illustrate the ranking method, below is a hypothetical example for a NPP examining the Relative risk ranking of five external events (EE). First step in the ranking method is to establish a relationship (ratio) between each of the EEs. Let (x) be a potential event occurrence value per year or unit time. If in DBEE report was found that the ratio of occurrence of "external flood" to "external fire" is twice as much in a given unit time then we put the appropriate value (2x) in the matrix table (see the shaded cell in table 5.1 next). In this example it is assumed that the ratio of external flood to other EEs (external fire, extreme wind, snow storm and Tsunami) is 1 : 2 : 1 : 3 : 10. Based on this ratio, the table below is completed. The "sum" is computed for each EE (i.e. sum of External Flood is 16x) and so on. Second step is evaluating the value of potential event occurrence (x). This is done by adding the all EEs "sum" terms and equating it unity. In this example the EE "Total Sum" is 58.5x which set equal to unit to find the value of (x) (such as 58.5x =1, therefore, x = 0.0171). In this example the value of (x) is found to be 0.0171.

The third step is evaluating each EE Relative risk by substituting the value of (x) in each EE's sum (i.e. the Relative risk of occurrence for External flood is 16x or 16*0.0171 = 0.27 or 27%). Table 5.1 and 5.2 show the summary of Relative risk ranking method for example above:

	External Flood	External Fire	Extreme Wind	Snow Storm	Tsunami	Sum
External Flood	-	2x	X	3x	10x	16x
External Fire	0.5	-	2x	3x	25x	30.5x
Extreme Wind	x	0.5x	-	2x	x	4.5x
Snow Storm	0.33x	0.33x	0.5x	-	5x	6.15x
Tsunami	0.1x	0.04x	X	0.2x	-	1.34x
					Total Sum	**58.5x**

Table 5.1 Relative Risk Ranking Method

Now, evaluating (x):

Total Sum =	**58.5 x**
58.5x = 1 (or 100%) --> x =	**0.0171**

Now, evaluating $\boldsymbol{P_e}$

EE Type	P_e	(%)
External Flood	16x 16*0.0171 = 0.27	27
External Fire	30.5x 30.5*0.0171 = 0.52	52
Extreme Wind	4.5x 4.5*0.0171 = 0.08	8
Snow Storm	6.15x 6.15*0.0171 = 0.11	11
Tsunami	1.34x 1.34*0.0171 = 0.02	2

Table 5.2 Relative Risk Ranking Summary

The purpose of the Relative risk ranking is to give proper weight when planning or evaluating mitigation plan. Based on the example above, it can be concluded that this hypothetical NPP is more likely to experience "External Fire" event (52%) than any other EE. Such information must be taking into consideration when designing the mitigation plan accordingly. The information from the relative risk ranking must drive the site's budgeting policy, EOPs, AOPs, SAMGs and emergency mitigation planning.

- **5.2.3 EMP Matrices: The Alpha-Factors: α_1, α_2, α_3, α_4**

The *EMP* assessment model presents four essential factors in an effort to design a comprehensive plan able to protect the NPP from EE consequences. Based on past NPP accidents and events such as the Fukushima, Japan accident in 2011 where human error, un-accessible emergency equipment (such as DEGs), communication failure, inadequate NPP site physical barriers as well as ineffective inherent safety systems were the main problems to contain and control the reactor core, stop propagation of radioactive (fuel) material into the surrounding environment and protect the public from one of the worst nuclear accidents in modern times. The alpha-factors (in the *EMP* model) are designed to illustrate the strengths and weaknesses of each of the mitigation plan areas. Proper quantification of the alpha-factors is key in accurate evaluation ***NPP Vulnerability***. Each alpha-factor is evaluated independently, see figure (5.1). Furthermore, in current presentation of the assessment model as per equation (5.1), the alpha factors have equal weight in the mitigation plant of NPP site. The absence of any alpha-factor (or minimal evaluated value) in the *EMP* assessment model represents a hazardous gap in the nuclear site's mitigation plan readiness and will drive the ***NPP Vulnerability*** factor to higher levels indicating NPP is potentially unsafe to mitigates EEs effectively.

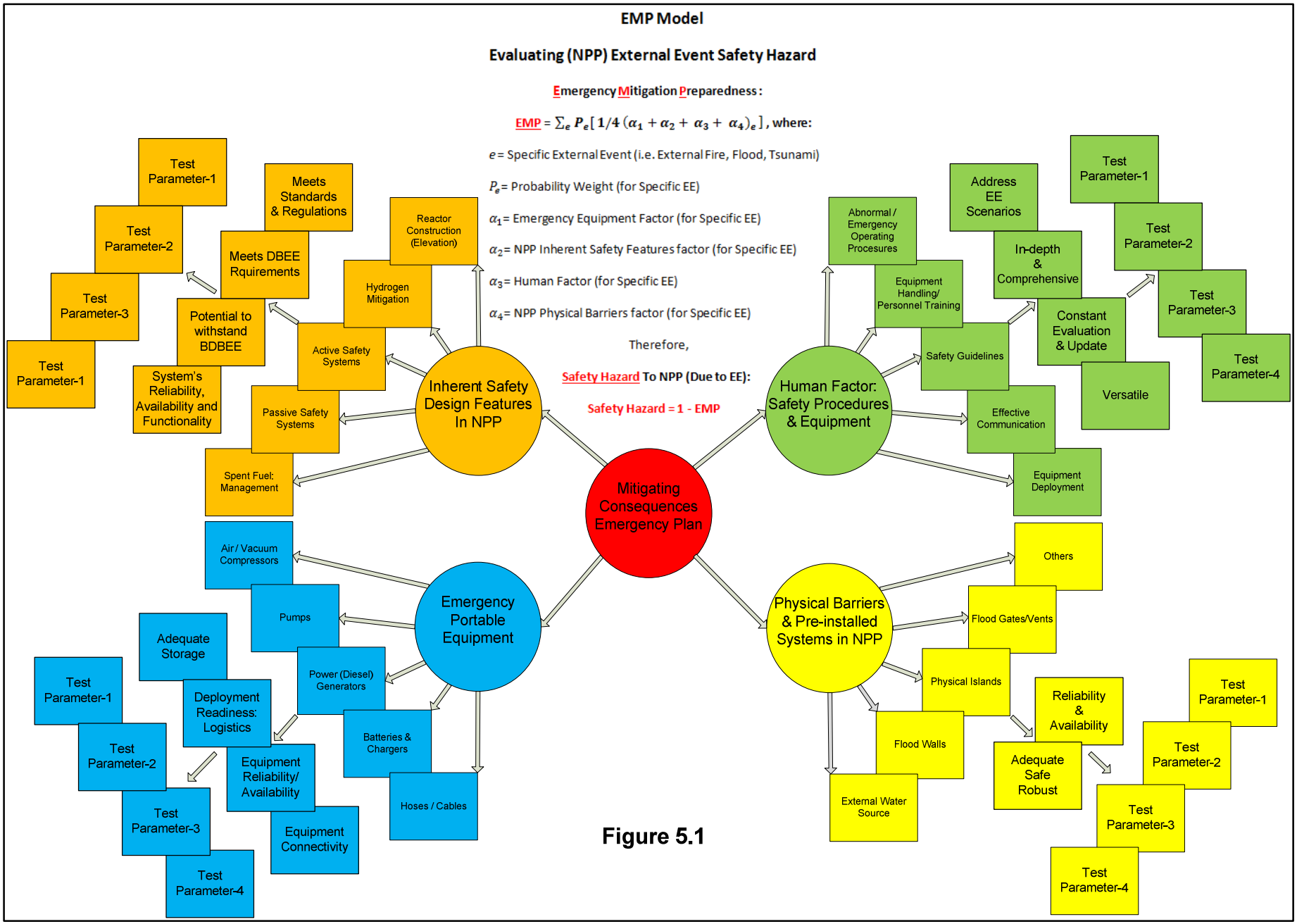
EMP Model
Evaluating (NPP) External Event Safety Hazard
Emergency Mitigation Preparedness:
EMP = $\sum_e P_e[1/4\,(\alpha_1+\alpha_2+\alpha_3+\alpha_4)_e]$, where:
e = Specific External Event (i.e. External Fire, Flood, Tsunami)
P_e = Probability Weight (for Specific EE)
α_1 = Emergency Equipment Factor (for Specific EE)
α_2 = NPP Inherent Safety Features factor (for Specific EE)
α_3 = Human Factor (for Specific EE)
α_4 = NPP Physical Barriers factor (for Specific EE)
Therefore,
Safety Hazard To NPP (Due to EE):
Safety Hazard = 1 - EMP
Mitigating Consequences Emergency Plan
Inherent Safety Design Features In NPP
Test Parameter-1
Test Parameter-2
Test Parameter-3
Test Parameter-1
Meets Standards & Regulations
Meets DBEE Rquirements
Reactor Construction (Elevation)
Hydrogen Mitigation
Potential to withstand BDBEE
Active Safety Systems
System's Reliability, Availability and Functionality
Passive Safety Systems
Spent Fuel: Management
Human Factor: Safety Procedures & Equipment
Abnormal / Emergency Operating Procesures
Address EE Scenarios
Test Parameter-1
Test Parameter-2
Test Parameter-3
Test Parameter-4
Equipment Handling/ Personnel Training
In-depth & Comprehensive
Constant Evaluation & Update
Safety Guidelines
Versatile
Effective Communication
Equipment Deployment
Emergency Portable Equipment
Air / Vacuum Compressors
Pumps
Adequate Storage
Power (Diesel) Generators
Deployment Readiness: Logistics
Batteries & Chargers
Test Parameter-1
Test Parameter-2
Test Parameter-3
Test Parameter-4
Equipment Reliability/ Availability
Hoses / Cables
Equipment Connectivity
Physical Barriers & Pre-installed Systems in NPP
Others
Flood Gates/Vents
Physical Islands
Flood Walls
External Water Source
Reliability & Availability
Adequate Safe Robust
Test Parameter-1
Test Parameter-2
Test Parameter-3
Test Parameter-4

Figure 5.1

- **5.2.4 Emergency Equipment Alpha Factor - α_1: Metric**

Emergency equipment is one of the main pillars in the *EMP* assessment model due to its significant role it employs during mitigating severe accidents. Immediate and prompt access to emergency equipment that is designed specifically to meet the EE challenges may in fact be the prime factor in managing, containing and controlling the reactor core in severe accident situations. The Fukushima accident is a great example that showed the importance and impact of emergency equipment to maintain reactor core integrity: the lack of EDGs required to cool, maintain and control the reactor core was one of the main reasons for core melt down to occur. The *EMP* assessment model values the importance of the Emergency Equipment in mitigating accidents and thus a specific factor alpha-1 (α_1) was designed to reflect this importance on the overall evaluation of the ***NPP Vulnerability***. Alpha-1 (α_1) factor reflects the availability and readiness in NPP to address EE; these emergency equipment are mostly portable, available on-site and off-site and suitable to address severe accidents and consequences caused by various EE scenarios. The Alpha-1 (α_1) is expandable depending on NPP needs: addressing new EE events, incorporating new equipment or meeting equipment safety guidelines. The first stage when computing the Alpha-1 (α_1) factor requires a thorough listing of all required emergency equipment for a specific site that are needed to mitigate potential severe accidents caused by a specific EE, as per the DBEE report. The second stage, in evaluating the alpha-1 factor (α_1), is establishing the required equipment characteristics and features to see if the selected emergency equipment for the specific EE will be adequate for the EE event. For instance, a typical list of emergency equipment required for during a Tsunami event would be, but not limited to the following:

- Air compressors & various types of pumps, EDGs
- Various machinery for loading, moving, towing and clearing roads
- Batteries /chargers / cables/ hoses
- Spare parts, tools, torches and other accessories
- Adequate (per EE) Personal Protective Equipment

The second step of the Alpha-1 quantification process is establishing parameters, as deemed fit by the NPP, to gauge the list of emergency equipment (first step). Possible evaluation can be based on the following characteristics criterion:

- Equipment adequate storage to withstand the specific EE
- Deployment readiness of equipment
- Equipment reliability/availability
- Equipment connectivity

In the third step of Alpha-1 evaluation, each of the criterions (from the second stage) will be further evaluated based on further sub-criterion and test parameters established by the NPP, IAEA or the industry. Following our examples, some of the test parameters for emergency equipments would be based on (see figure 5.2):

- In-depth defense: barriers by distance, elevation, seismic, flood, wind and fire
- Does storage meet IAEA standards for the specific EE
- Frequent equipment testing, evaluation, analysis, handling and upgrade
- Personnel training on equipment, procedures
- Flexible equipment connectivity, readiness and deployment

The test and evaluation criterion can be standardized for each NPP and/or be flexible to reflect the continued update in nuclear safety research; thus making the alpha-1 factor fluid and current. The maximum value of the alpha-1 factor is 1 (or 100%) for each EE. In each stage, the weight is equally divided within its sub-category or within its test parameters thus making each step equally valuable. Certain values are given for each specific task or test parameter during the computing *all* Alpha factors is as below:

Task or Test Parameter	Credit
Fully Completed Task/Test	**1.0**
In Progress Task/Test	**0.5**
Task is not initiated	**0.0**
Not Applicable	**n/a**

Table 5.3 Task / Test Parameter Credits

In the current assessment methodology of *EMP*, respective test categories and test parameters are considered independent and can be performed simultaneously of each other. However, if a case exists where a direct link is established between two or more categories or test parameters the *EMP* assessment model can easily be adjusted to accommodate such criteria.

Alpha-1: Emergency Equipment Factor Evaluation Process

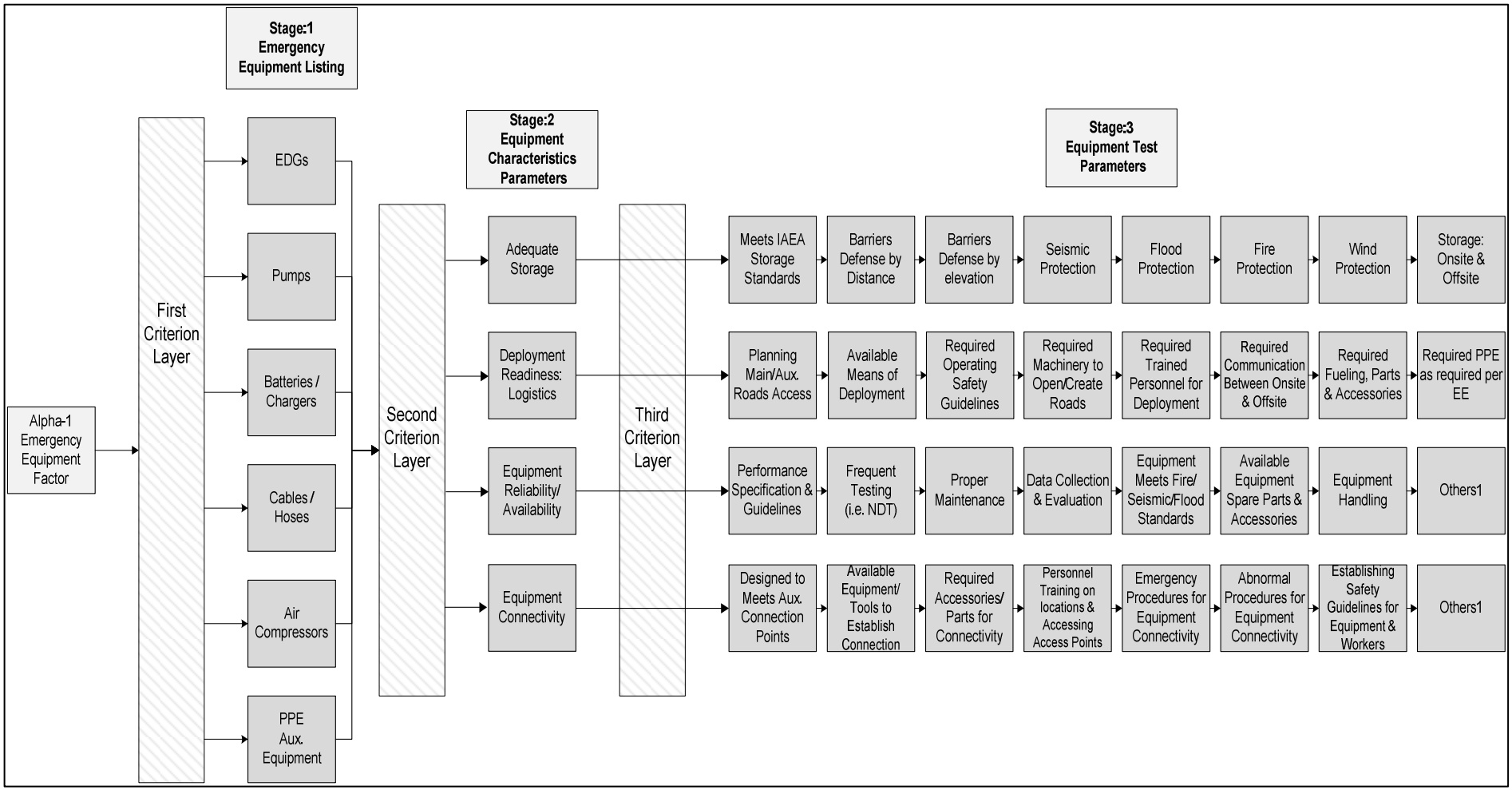

Figure 5.2

▪ 5.2.5 NPP Inherent Safety Features factor: α_2: Metric

NPP is designed by engineers to operate with higher safety fashion compared to any other plant due to potential harmful radioactive material involved in the process of energy production as well as due to potential devastation in severe accidents (historically) to the surrounding environment and community at large. For this reason, NPP is equipped with a multiply defense safety systems to insure control and containment of Reactor Core (RC). These systems are divided into: (1) Safe Containment systems (2) RC Active Safety systems (3) RC Passive Safety Systems (4) Hydrogen Mitigation systems and (5) Spent Fuel Management. *EMP* assessment model presents the Alpha-2 factor ($\boldsymbol{\alpha_2}$) to address the importance of NPP safety systems in mitigating potential accidents and reducing overall NPP vulnerability due to EE. Similar to earlier factor Alpha-1, the approach is analytical to realistic and accurate quantification as seen in figure 5.3. Functional NPP inherent safety systems act autonomously and independently of each other in a severe accident situation. There are wide arrays of available systems currently used in the nuclear generation industry, such as:

- Safe Containment: Containment of radioactive material is a primary starting point to any containment plan such as (1) the use of oxide fuel ceramic (Uranium Oxide) for higher thermal and physical fuel stability (2) pallet type fuel (in CANDU reactors) which adds resistance to fuel deformation (3) fuel housing or high pressure tubing made of Zirconium (Zr) metal adds the first protection layer from fuel leakage (4) low/high pressure vessel containment adds a secondary layer of radioactive material leakage (5) containment building and vacuum building acts as a

last resort for radioactive containment and spread (6) vacuum system/buildings for temporary containment and (7) multi-pressure reliefs with radioactive multi-stage filtration.

- RC active safety systems: Active systems require external AC power to operate. Generally, active systems such as UHS are designed to provide forced cooling in severe accident events to avoid RC damage. Typical active systems are (1) primary cooling system which (light/heavy water coolant) removes heat generated within the fuel in the RC (2) secondary cooling system which (ordinary water) removes heat from primary coolant and aids in generating steam within the SG (3) third cooling system which (sea/lake/river water) removes heat from steam and aids in sub cooling the steam and (4) various external/auxiliary water reservoir pumping systems for emergency reactor cooling and coolant supply.
- RC passive safety systems: typically, these systems require an external power source to perform its functions. Usually passive systems utilize natural (or internal potential) forces to operate and provide cooling to RC such as (1) gravity drain tank (2) containment pressure suppression pools (3) sump natural circulation (4) passive containment spray (5) pre-pressurized core flooding tanks or accumulators (6) passively cooed steam generator natural circulation and (7) Isolation Condensers and much more.
- Hydrogen mitigation: is definitely a critical component in mitigating severe accidents since low combustible Hydrogen energy is a major safety concern in the event of no or poor cooling of the RC. In the recent Fukushima, Japan (2011) accident, lack of core cooling caused the coolant to evaporate into steam. The high core temperature acted as a good catalyst for the Zirconium to oxidize thus removing the oxygen from the steam and increasing the presence of Hydrogen gas in the reactor vessel which led shortly thereafter to a major Hydrogen explosion in buildings

number 1 and 3. Typical hydrogen management plans include (1) pre-inertization with nitrogen (2) post-inertization with nitrogen (3) Passive Autocatalytic Recombiners -PAR- in large dry PWR containments and (4) Igniters such as Glow Plugs, Spark Igniters, Catalytic Igniters and Spontaneous Igniters.

- Spent fuel management: unfortunately, the nuclear power plants globally suffer from spent fuel constipation movement. NPP possess significant quantities of irradiated fuel onsite in storage for no reason but lack safer nuclear waste management options. Decay heat from irradiated fuel bay is not significant compared to the reactor core, but spent fuel pools have limited cooling resources compared to the reactor core. Thus, provision must be made to restore cooling and heat removal to spent fuel bay post a severe accident. Forced cooling, portable pumps, cooling equipment and access to a large body of water are part of defence in depth to manage heat decay of irradiated fuel bays.

The first stage when computing the Alpha-2 (α_2) factor requires a complete listing of all required safety systems in the NPP such as site construction, active safety systems, passive safety systems, Hydrogen mitigation and spent fuel management. The second stage, in evaluating the alpha-2 factor (α_2), is determining the safety characteristics for the safety system to perform in order to withstand a severe accident scenario caused by a specific EE. The third stage states the test and procedures parameters to evaluate; see figure 5.3 for the evaluation process of NPP inherent safety systems.

Alpha-2: NPP Inherent Safety Systems Factor Evaluation Process

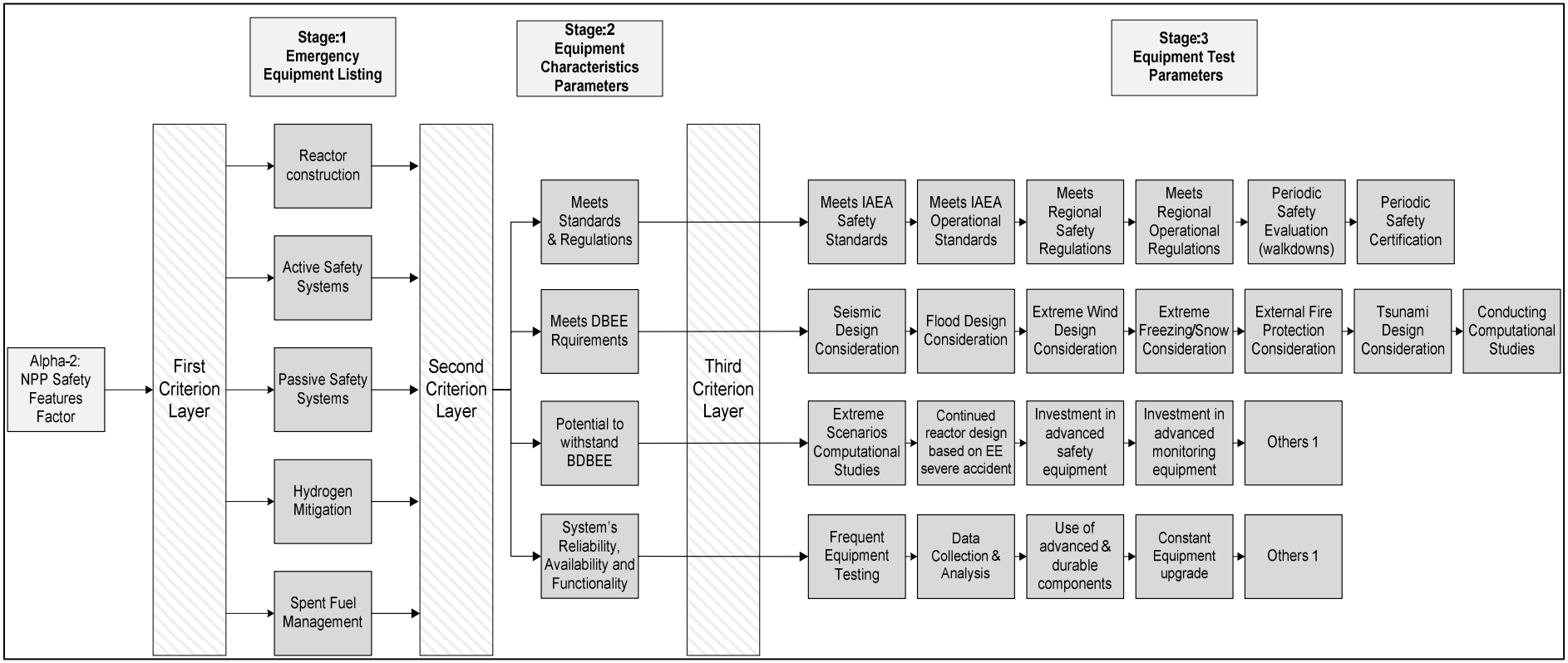

Figure 5.3

- **5.2.6 Human Factor α_3: Metric**

The Three Mile Island accident in 1979 was the driving force behind the need to introduce the Human Reliability Analysis (HRA) factor in evaluating safety risk in NPP. The three major nuclear accidents: Three Mile Island (1979), Chernobyl (1986) and Fukushima (2011) are arguably caused to some extent by human error: lack adherence to safety and test procedures as well as poor plant safety culture. As a result, Safety and PRA modeling should include both deterministic and probabilistic HRA in their analysis and assessment to quantify more accurately the risk in NPP. However, current assessment does ignore many human interfacing areas in the assessment model. Mitigating effective emergency planning in the face of the after math of EE or severe accident, the *EMP* model does account for Human Factor Alpha-3 ($\boldsymbol{\alpha_3}$) and considers it a main pillar in emergency response planning. The Alpha-3 factor quantifies a wide range of human interfaces with emergency planning elements such as:

- Improvement and updates on safety guidelines and emergency operating procedures
- Personnel Assets
- Communication
- Equipment Deployment Readiness

In the wake of the Fukushima accident, it was realized the need to improve safety guidelines and emergency operating procedures in all NPPs worldwide to address potentially similar accidents. The lack of safety culture and no effective or comprehensive approach in accident mitigation is no longer feasible as public safety is becoming a priority and a need to be maintained. NPP is required to plan for all possible scenarios for internal events, external

events, and potential multi-unit failures/accidents. As a result, there is always a need to continue updating plant safety guidelines as more information is available to protect the workers and the public. Emergency operating procedures for each severe accident caused by an internal event or external event must be addressed, constantly evaluated and simplified, regular training and execution should also be mandated. Trained and experience workers are key stones in executing a mitigation plan with confidence. Thus, reliance on constant personnel training, knowledge update, readiness to deploy equipment and having multiple onsite and offsite emergency teams ready to execute emergency procedures is key.

The need for effective communication between onsite and offsite personnel is integral to any effective mitigation plan execution. Thus multiple technologies is required to compensate for any potential scenario and event such as having communication teams, powering communication equipment, radio, satellite, cellular and telephone equipment. Similar to earlier factors, the Human factor Alpha-3 (α_3) is evaluated based on three layer criterion and test parameters as seen in figure 5.4.

Alpha-3: Human Factor Evaluation Process

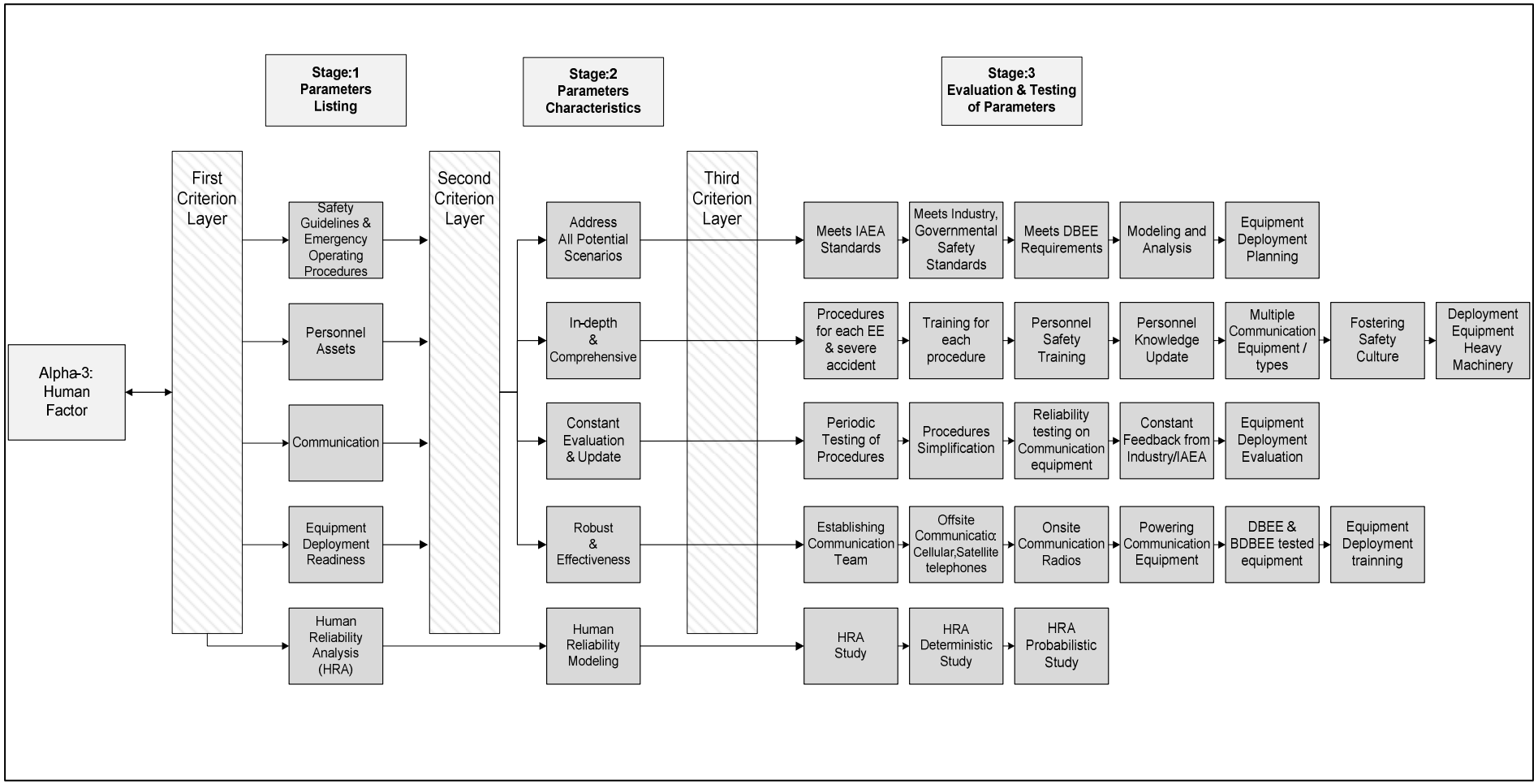

Figure 5.4

▪ 5.2.7 NPP Physical Barriers factor α_4: Metric

Most NPPs in the world are built near a large water body such as rivers, lakes and oceans. DBEE reports quantify potential hazards and damage to the site caused by a large body of water due to events such as massive flooding and Tsunami. Thus a need for physical barriers to protect the site from external events and limit potential damages is paramount and necessary. However, poor design and planning of such physical barriers can have a catastrophic impact on the NPP operation and safety. The Fukushima accident is a good example where current design of flood walls was adequate to sustain a massive earthquake but not to with stand a powerful Tsunami. The result was massive flooding of the NPP rendering all emergency equipment on site inoperable.

The *EMP* assessment model introduces Physical Barriers factor, Alpha-4 (α_4), into the quantification of the overall NPP emergency mitigation planning. Unlike the long list of emergency equipment required by the NPP to mitigate emergency, physical barriers in NPP are limited such as:

- Flood (Sea) Walls
- External Water Source
- Physical Islands
- Flood Gates/Vents
- Drainage System

Similar to earlier factors, the NPP Physical Barriers factor, Alpha-4 (α_4) and other pre-installed barrier systems are evaluated based on three layer criterion /test parameters as in figure 5.5.

Alpha-4: NPP Physical Barriers Evaluation Process

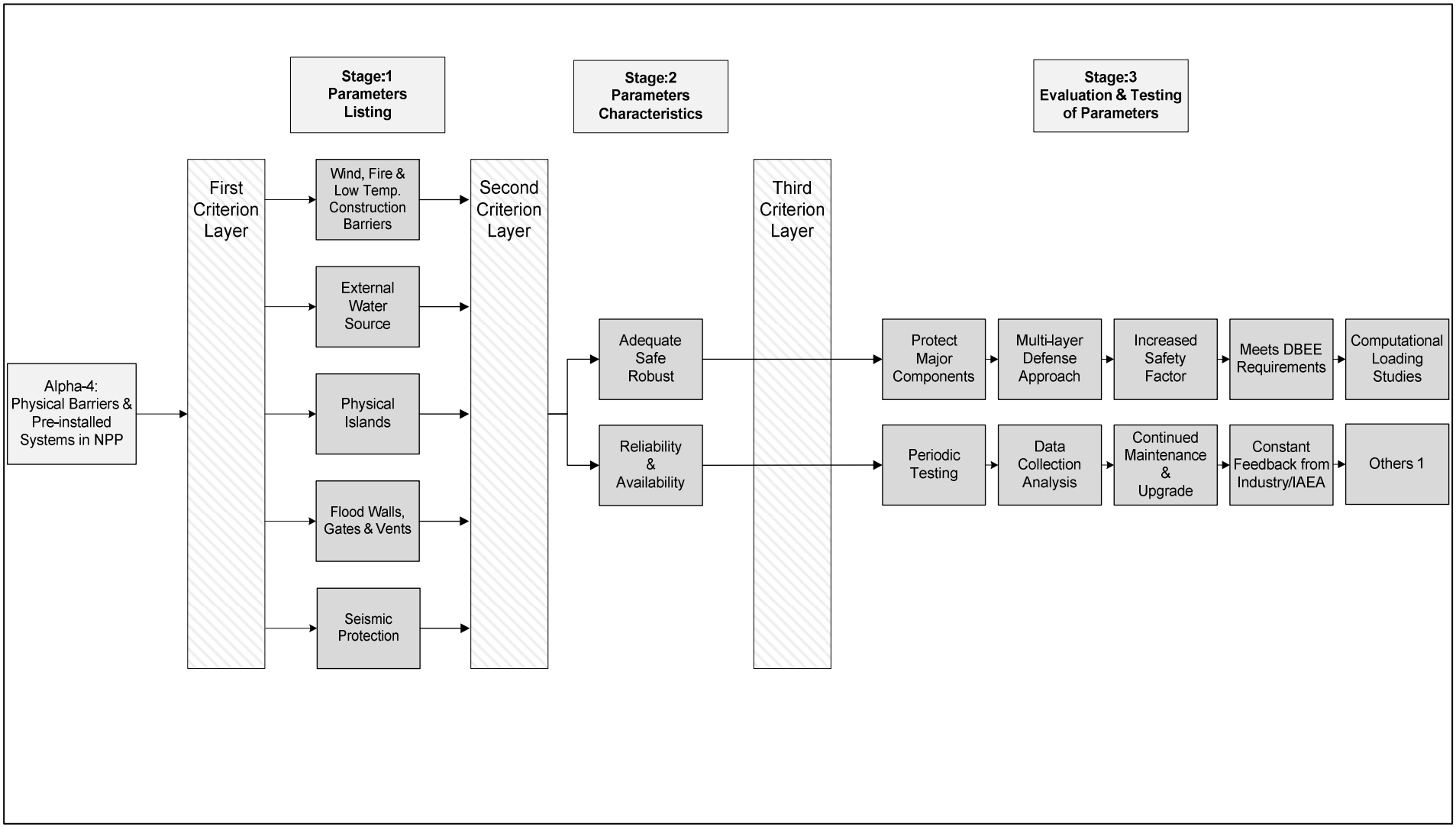

Figure 5.5

5.3 NPP Vulnerability Factor

By now, the relative risk ranking for potential EEs based on (site specific) DBEE report are evaluated; further, all Alpha-factors (α_1, α_2, α_3, α_4) are computed for each EE in DBEE. The next step is evaluating the *EMP* factor as in equation (5.1), such as:

$$\textbf{EMP} = \sum_e \boldsymbol{P_e}[\,\mathbf{1/4}\,(\boldsymbol{\alpha_1} + \boldsymbol{\alpha_2} + \boldsymbol{\alpha_3} + \boldsymbol{\alpha_4})_e\,] \qquad (5.1)$$

The *EMP* factor provides the mitigating consequences readiness level for a NPP to address EEs based on DBEE report and severe accidents. The ***NPP Vulnerability*** factor is a quantity required by the NPP to evaluate the overall potential NPP vulnerability due to lack of mitigation readiness to contain and control severe accidents and EE consequences. Thus, ***NPP Vulnerability*** is defined as:

$$\textbf{\textit{NPP Vulnerability}} = \mathbf{1} - \textbf{EMP} \qquad (5.2)$$

NPP Vulnerability factor is an added value to any plant safety planning, strategy and policy to combat EE. Also, NPP Vulnerability analysis can be used as an indicator to detail areas of short coming in the safety and mitigation planning by the NPP. The *EMP* assessment model provides a bench mark quantitative assessment of EE mitigation readiness and evaluation of vulnerability to the site, workers, environment and the surrounding community.

The general *EMP* assessment model summary is represented in figure 5.6 using Boolean Logic - fault tree diagram. For illustration only, multiple External Events such as Tsunami, External Fire, External Flooding, Extreme Wind and Snow Storm events are incorporated in the logic diagram. More External Events can easily be added as required by the DBEE report for a specific NPP.

5.4 Multiple EE Logic Representation of EMP Assessment Model: Summary

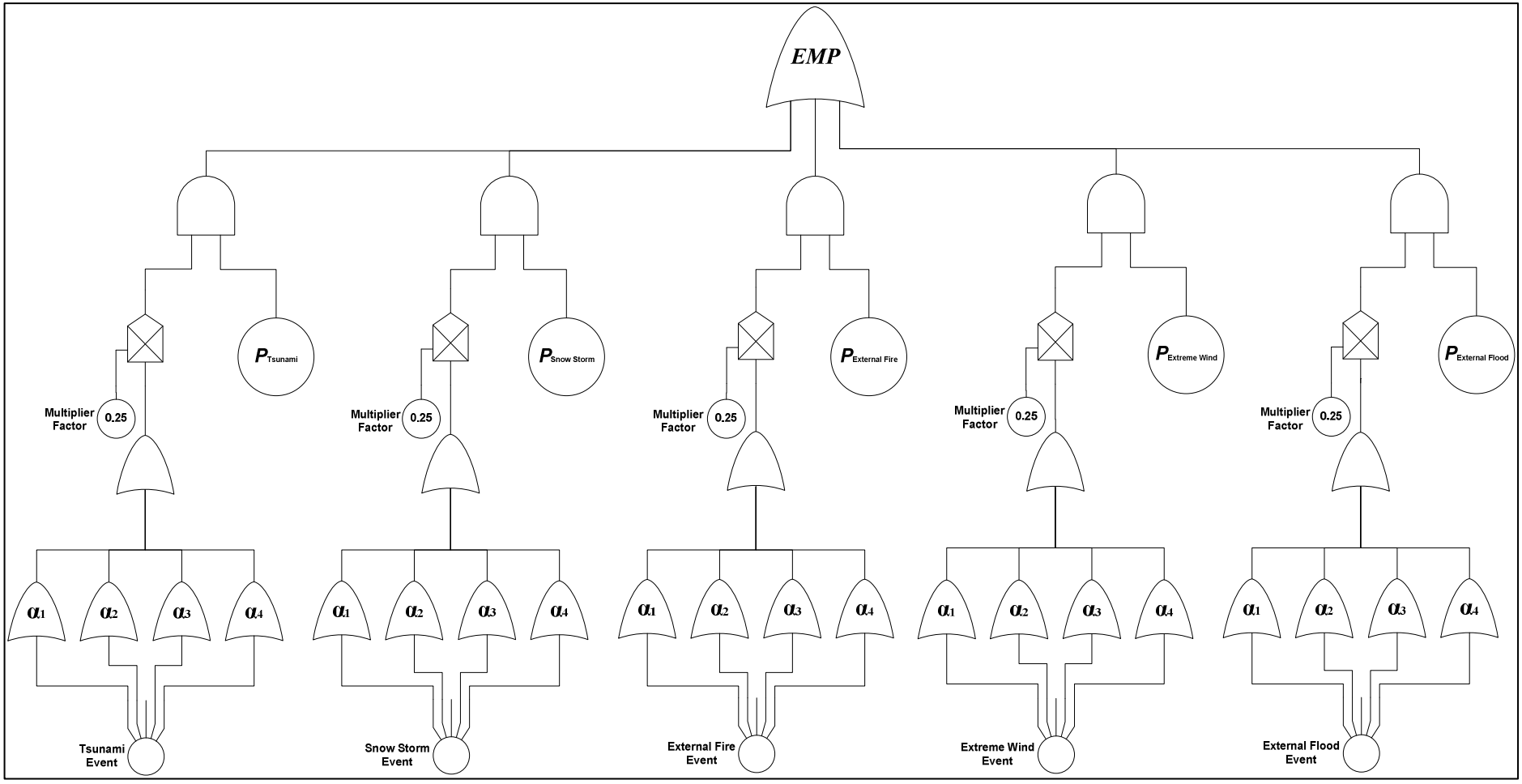

Figure 5.6

CHAPTER 6

Fukushima Accident: Case Study & Analysis

6.1 Fukushima Daiichi NPP Accident

On March 11th, 2011 a large unexpected Tsunami hit the Fukushima Daiichi nuclear plant. The waves knocked down the grid power supply to the plant which led to the shutdown of the reactor cooling system. Reactor unit #1 experienced the first core meltdown roughly 10 hours after the earthquake and consequently a hydrogen explosion. Reactor core #3 was also badly damaged - core meltdown - like unit #1 and experienced hydrogen explosion 3-days later on March 14th, 2011. Reactor unit #2 coolant system was active for the first couple of hours then stopped and there were no way for water to be replenished in the reactor core. Further, due to the high internal steam pressure, water started leaking out of the reactor vessel and there was no possible way to inject water into the reactor to cool the core down. The decay heat from the fuel rod continued to produce heat causing coolant with the reactor core to evaporate and thus exposing fuel rods which lead to a complete and uncontrolled core meltdown. There are 8-Safety Relief (SR) valves found in unit#2 used for emergency to release steam pressure from inner core vessel housed within the primary containment vessel. SR valves are controlled remotely by the operator and require battery power to release -Nitrogen gas-a pilot signal to overcome back pressure from the core vessel in order to open the SR valve. Unfortunately, the SR valves were not responding and pressure within the reactor core continued to rise, not to mention that Dry-Well venting as a last resort to relief vessel's pressure also failed to bring the

pressure down. Eventually, on March 14th, melted fuel penetrated the bottom of the reactor vessel and leaked into the primary containment vessel and resulting in the final explosion of the containment vessel.

6.2 Case Study - 1

EMP and *NPP Vulnerability* Evaluation due to Single External Event "Tsunami"

Based on the events that took place during the Fukushima NPP accident in 2011, an *EMP* assessment will be attempted below. In this example, only the Tsunami event is evaluated in depth (see figure 6.1 below). Alpha factors α_1, α_2, α_3 and α_4 are assessed based on the events transpired and knowledge known thus far about the 2011 Fukushima nuclear accident.

Alpha factors are evaluated based on events occurred during the Fukushima accident. Below are some facts used for the ***EMP*** and ***NPP Vulnerability*** assessment:

- Emergency backup batteries were flooded and thus not available to operate important components to control the reactor core temperature. Additional offsite batteries were also not immediately available.
- EDGs were lost due to Tsunami and thus not available to provide the NPP site with needed power to restore RC control and temperature

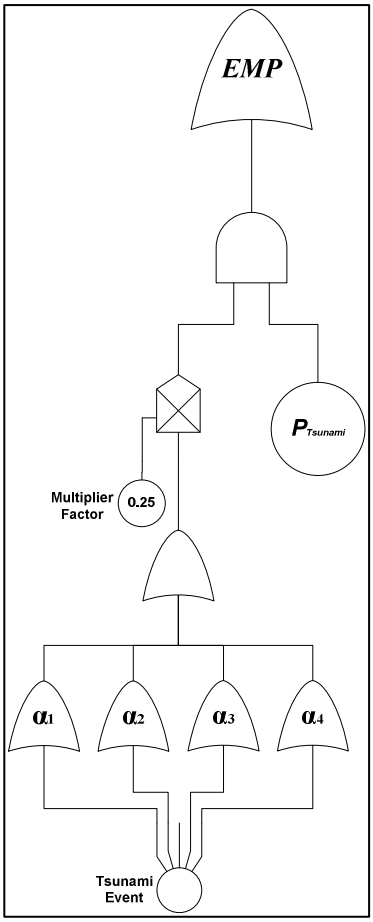

Figure 6.1 Logic Diagram for *Tsunami EMP*

- Operators and the utility company showed lack of clear communication about the status of the reactor cores and how to control it. No immediate technical assistance was provided to the operators to open the vent valve or SR valves in a timely manner.
- Construction of the reactor site was based on three safety classes that varied in structure strength. The air piping system is built based on C-class - lowest structure strength - thus air supply did not sustain the Tsunami and rendered it not available.

6.2.1 Alpha-1: Emergency Equipment: Evaluation Process Evaluation

The evaluation process for Alpha-1 is summarized in table 6.1 (below). First, a complete list of emergency equipment is compiled such as EDGs, water pump, air compressors, batteries/chargers, cables/hoses, spare parts and finally tools and accessories. Second, applicable equipment criteria is established such as adequate storage, deployment readiness, equipment reliability and equipment connectivity. Third and final step is formulating test parameters for each item listed in step two. Each test is credited as discussed in "Task/Test Parameter Credits" table 5.3 in chapter 5:

Task or Test Parameter	Credit
Fully Completed Task/Test	**1.0**
In Progress Task/Test	**0.5**
Task is not initiated	**0.0**
Not Applicable	**n/a**

The evaluation of "Adequate Storage" is summarized below. The weighted average is calculated in the last row and then inserted in the second column of Alpha-1 Summary table 6.5 below.

Adequate Storage	**EDGs**	**PUMPs**	**Air Comp.**	**Batteries**	**Cables/ Hoses**	**Spare Parts**	**Tools**
Barriers by distance	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Barriers by elevation	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Seismic Protection	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Flood Protection	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Wind Protection	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Fire Protection	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Meets IAEA Standards	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Meets DBEE / BDBEE	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Equipment Storage	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Weight Average	**0.67**	**0.67**	**0.67**	**0.67**	**0.67**	**0.67**	**0.67**

Table 6.1 Evaluation Process for Adequate Storage (values inserted in column-2 in table 6.5)

The evaluation of "Deployment Readiness" is summarized below. The weighted average is calculated in the last row and then inserted in the third column of Alpha-1 Summary table 6.5.

Deployment Readiness & Logistics	**EDGs**	**PUMPs**	**Air Comp.**	**Batteries**	**Cables/ Hoses**	**Spare Parts**	**Tools**
Planning Access Roads	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Means of Deployment	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Required Operating Safety Guidelines	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Required Machinery to Open/Create Roads	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Trained Personnel for Deployment	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Required Communication Be Between Onsite & Offsite	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Fuel, Parts & Accessories	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Required PPE as per EE	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Weight Average	**0.63**	**0.63**	**0.63**	**0.63**	**0.63**	**0.63**	**0.63**

Table 6.2 Evaluation Process for Deployment Readiness (value inserted incolumn-3 in table 6.5)

The evaluation of "Equipment Reliability" is summarized below. The weighted average is calculated in the last row and then inserted in the forth column of Alpha-1 Summary table 6.5.

Equipment Reliability & Availability	**EDGs**	**PUMPs**	**Air Comp.**	**Batteries**	**Cables/ Hoses**	**Spare Parts**	**Tools**
Performance, Specification & Guidelines	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Frequent Testing (NDT)	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Proper Maintenance	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Data Collection & Evaluation	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Equipment meets fire/flood/seismic standards	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Available Equipment Spare Parts/Accessories	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Equipment Handling	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Redundant Equipment/Systems	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Weight Average	**0.94**	**0.94**	**0.94**	**0.94**	**0.94**	**0.94**	**0.94**

Table 6.3 Evaluation Process for Equipment Reliability (values inserted in column-4 in table 6.5)

The evaluation of "Deployment Readiness" is summarized below. The weighted average is calculated in the last row and then inserted in the third column of Alpha-1 Summary table 6.5.

Equipment Connectivity	**EDGs**	**PUMPs**	**Air Comp.**	**Batteries**	**Cables/ Hoses**	**Spare Parts**	**Tools**
Designed to Meets Aux. Connection Points	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Available Equipment/Tools to Establish Connection	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Accessories/Parts for Connectivity	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Personnel Training on locations & Accessing Access Points	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Emergency Procedures for Equipment Connectivity	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Abnormal Procedures for Equipment Connectivity	0.50	0.50	0.50	0.50	0.50	0.50	0.50
Establishing Safety Guidelines for Equipment & Workers	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Weight Average	**0.57**	**0.57**	**0.57**	**0.57**	**0.57**	**0.57**	**0.57**

Table 6.4 Evaluation Process for Equipment Connectivity (values inserted in column-5 in table 6.5)

Results from tables 6.1 through 6.4 are imported into table 6.5 (below). "Readiness Average" is computed per each "Emergency Equipment". And finally the mean for "Readiness Average" for the entire equipment list is evaluated to be at 0.7 which corresponds to Alpha-1 value.

Alpha-1: Emergency Equipment Evaluation	*Adequate Storage*	*Deployment Readiness*	*Reliability*	*Connectivity*	Readiness Average
EDGs	0.67	0.63	0.94	0.57	0.70
Pumps	0.67	0.63	0.94	0.57	0.70
Air Compressors	0.67	0.63	0.94	0.57	0.70
Batteries/Chargers	0.67	0.63	0.94	0.57	0.70
Cables / Hoses	0.67	0.63	0.94	0.57	0.70
Spare Parts	0.67	0.63	0.94	0.57	0.70
Tools, Accessories & PPE	0.67	0.63	0.94	0.57	0.70
					0.70

Table 6.5 Alpha-1 Evaluation Summary

6.2.2 Alpha-2: Safety Systems and Features in NPP Evaluation

The evaluation process for Alpha-2 is summarized in table 6.10 (below). First, a list of NPP safety features is compiled such as reactor construction, active safety systems, passive safety systems, Hydrogen mitigation and spent fuel management. Second, applicable criteria is established such as meets the standards and regulations, meets BDEE requirements, Potential to withstand BDBEE and system reliability and availability. Third and final step is formulating test parameters for each item listed in step two. Each test is credited as discussed in "Task/Test Parameter Credits" table 5.3 in chapter 5.

The evaluation of "Meets Standards & Regulations" is summarized below. The weighted average is calculated in the last row and then inserted in the second column of Alpha-2 Summary table 6.10 below.

Meets Standards & Regulations	**Reactor construction**	**Active Safety Systems**	**Passive Safety Systems**	**Hydrogen Mitigation**	**Spent Fuel Management**
Meets IAEA Safety Standards	1.00	1.00	1.00	1.00	1.00
Meets IAEA Operational Standards	1.00	1.00	1.00	1.00	1.00
Meets Regional Safety Regulations	1.00	1.00	1.00	1.00	1.00
Meets Regional Operational Regulations	1.00	1.00	1.00	1.00	1.00
Periodic Safety Evaluation	1.00	1.00	1.00	1.00	1.00
Periodic Safety Certification	1.00	1.00	1.00	1.00	1.00
Weight Average	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**

Table 6.6 Evaluation Process for "Meets Standards & Regulations"
(values are inserted in column-2 in table 6.10)

The evaluation of "Meets BDEE Requirements" is summarized below. The weighted average is calculated in the last row and then inserted in the third column of Alpha-2 Summary table 6.10.

Meets DBEE Requirements	**Reactor construction**	**Active Safety Systems**	**Passive Safety Systems**	**Hydrogen Mitigation**	**Spent Fuel Management**
Seismic Design Consideration	1.00	1.00	1.00	1.00	1.00
Flood Design Consideration	0.00	0.00	0.00	0.00	0.00
Extreme Wind Design Consideration	1.00	1.00	1.00	1.00	1.00
Extreme Freezing/Snow Design Consideration	n/a	n/a	n/a	n/a	n/a
External Fire Protection Design Consideration	1.00	1.00	1.00	1.00	1.00
Tsunami Design Consideration	0.50	0.50	0.50	0.50	0.50
Conducting Computational Studies	0.50	0.50	0.50	0.50	0.50
Weight Average	**0.67**	**0.67**	**0.67**	**0.67**	**0.67**

Table 6.7 Evaluation Process for "Meets BDEE Requirements"
(values are inserted in column-3 in table 6.10)

The evaluation of "Potential to withstand BDBEE" is summarized below. The weighted average is calculated in the last row and then inserted in the fourth column of Alpha-2 Summary table 6.10.

Potential to withstand BDBEE	**Reactor construction**	**Active Safety Systems**	**Passive Safety Systems**	**Hydrogen Mitigation**	**Spent Fuel Management**
Extreme Scenarios Computational Studies	0.50	0.50	0.50	0.50	0.50
Reactor design based on EE severe accident	n/a	n/a	n/a	n/a	n/a
Investment in advanced safety equipment	1.00	1.00	1.00	1.00	1.00
Investment in advanced monitoring equipment	1.00	1.00	1.00	1.00	1.00
Weight Average	**0.83**	**0.83**	**0.83**	**0.83**	**0.83**

Table 6.8 Evaluation Process for "Potential to withstand BDBEE"
(values are inserted in column-4 in table 6.10)

The evaluation of "Systems Reliability & Availability" is summarized below. The weighted average is calculated in the last row and then inserted in the fifth column of Alpha-2 Summary table 6.10.

Reliability & Availability	**Reactor construction**	**Active Safety Systems**	**Passive Safety Systems**	**Hydrogen Mitigation**	**Spent Fuel Management**
Frequent Equipment Testing	1.00	1.00	1.00	1.00	1.00
Data Collection & Analysis	1.00	1.00	1.00	1.00	1.00
Collection & Analysis	1.00	1.00	1.00	1.00	1.00
Use of advanced & durable components	1.00	1.00	1.00	1.00	1.00
Constant Equipment Upgrade/Advancement	1.00	1.00	1.00	1.00	1.00
Weight Average	**1.00**	**1.00**	**1.00**	**1.00**	**1.00**

Table 6.9 Evaluation Process for " Systems Reliability & Availability "
(values are inserted in column-5 in table 6.10)

Results from tables 6.6 through 6.9 are imported into table 6.10 (below). "Readiness Average" is computed per each criteria. And finally the mean for "Readiness Average" for the entire list is evaluated to be at 0.88 which corresponds to Alpha-2 value.

Alpha-2: NPP Safety Features Evaluation	***Meets Standards & Regulations***	***Meets DBEE Requirements***	***Potential to withstand BDBEE***	***Reliability & Availability***	***Readiness (Average)***
Reactor construction	1.00	0.67	0.83	1.00	0.88
Active Safety Systems	1.00	0.67	0.83	1.00	0.88
Passive Safety Systems	1.00	0.67	0.83	1.00	0.88
Hydrogen Mitigation	1.00	0.67	0.83	1.00	0.88
Spent Fuel Management	1.00	0.67	0.83	1.00	0.88
			Table 6.10 Alpha 2 Evaluation Summary		**0.88**

6.2.3 Alpha-3: Human Factor Evaluation

The evaluation process for Alpha-3 is summarized in table 6.16 (below). First, a list of safety guidelines/EOP/AOP, personnel assets, communication, equipment deployment readiness and human reliability analysis (HRA) is established. Second, applicable criteria is established such as addressing all potential EE scenarios, comprehensiveness, Evaluation & Update, Effectiveness and Human reliability modeling. Third and final step is formulating test parameters for each item listed in step two. Each test is credited as discussed in "Task/Test Parameter Credits" table 5.3 in chapter 5.

The evaluation of "Addressing all potential EE scenarios " is summarized below. The weighted average is calculated in the last row and then inserted in the second column of Alpha-3 Summary table 6.16 below.

Address All Potential Scenarios	**Safety Guidelines & Procedures**	**Personnel Assets**	**Communi-cation**	**Equipment Deployment Readiness**	**Human Reliability Analysis**
Meets IAEA Standards	1.00	1.00	1.00	0.00	0.50
Meets Industry, Governmental Safety Standards	1.00	1.00	1.00	0.00	0.50
Meets DBEE Requirements	0.50	1.00	1.00	0.00	0.50
Modeling and Analysis	n/a	n/a	n/a	n/a	0.50
Equipment Deployment Planning	n/a	0.50	0.50	0.50	n/a
Weight Average	**0.83**	**0.88**	**0.88**	**0.13**	**0.50**

Table 6.11 Evaluation Process for "Addressing all potential EE scenarios"
(values are inserted in column-2 in table 6.16)

The evaluation of "Comprehensiveness" criteria is summarized below. The weighted average is calculated in the last row and then inserted in the third column of Alpha-3 Summary table 6.16.

Comprehensive	**Safety Guidelines & Procedures**	**Personnel Assets**	**Communication**	**Equipment Deployment Readiness**	**Human Reliability Analysis**
Procedures for EE/severe accident	1.00	1.00	1.00	1.00	1.00
Training for each procedure	n/a	n/a	1.00	1.00	n/a
Personnel Safety Training	1.00	1.00	1.00	1.00	n/a
Personnel Knowledge Update	1.00	1.00	1.00	1.00	n/a
Communication Equipment / types	n/a	n/a	1.00	1.00	n/a
Fostering Safety Culture	1.00	1.00	1.00	1.00	1.00
Equipment & Machinery Deployment	n/a	n/a	0.50	0.50	n/a
Weight Average	**1.00**	**1.00**	**0.93**	**0.93**	**1.00**

Table 6.12 Evaluation Process for "Comprehensiveness"
(values are inserted in column-3 in table 6.16)

The evaluation of " Constant Evaluation& Update " is summarized below. The weighted average is calculated in the last row and then inserted in the fourth column of Alpha-3 Summary table 6.16.

Constant Evaluation& Update	**Safety Guidelines & Procedures**	**Personnel Assets**	**Communication**	**Equipment Deployment Readiness**	**Human Reliability Analysis**
Periodic Testing of Procedures	1.00	1.00	1.00	1.00	0.50
Procedures Simplification	1.00	1.00	1.00	1.00	1.00
Reliability testing on Communication equipment	n/a	n/a	1.00	n/a	n/a
Constant Feedback from Industry/IAEA	1.00	1.00	1.00	1.00	1.00
Equipment Deployment Evaluation	n/a	n/a	1.00	1.00	n/a
Weight Average	**1.00**	**1.00**	**1.00**	**1.00**	**0.83**

Table 6.13 Evaluation Process for " Constant Evaluation& Update "
(values are inserted in column-4 in table 6.16)

The evaluation of " Effectiveness " is summarized below. The weighted average is calculated in the last row and then inserted in the fifth column of Alpha-3 Summary table 6.16.

Effectiveness	**Safety Guidelines & Procedures**	**Personnel Assets**	**Communication**	**Equipment Deployment Readiness**	**Human Reliability Analysis**
Communication Team	n/a	1.00	1.00	1.00	1.00
Offsite Communication: Cells & telephones	1.00	1.00	1.00	1.00	1.00
Onsite Radios	1.00	1.00	1.00	1.00	1.00
Powering Communication Equipment	1.00	1.00	1.00	1.00	1.00
DBEE & BDBEE tested equipment	1.00	1.00	1.00	1.00	0.50
Equipment Deployment training	1.00	1.00	1.00	1.00	1.00
Weight Average	**1.00**	**1.00**	**1.00**	**1.00**	**0.92**

Table 6.14 Evaluation Process for " Effectiveness "
(values are inserted in column-5 in table 6.16)

The evaluation of "HRA Modeling" is summarized below. The weighted average is calculated in the last row and then inserted in the sixth column of Alpha-3 Summary table 6.16.

HRA Modeling	**Safety Guidelines & Procedures**	**Personnel Assets**	**Communication**	**Equipment Deployment Readiness**	**Human Reliability Analysis**
HRA Studies	0.50	0.50	0.50	0.50	0.50
Deterministic Approach	0.50	0.50	0.50	0.50	0.50
Probabilistic Approach	0.50	0.50	0.50	0.50	0.50
Weight Average	**0.50**	**0.50**	**0.50**	**0.50**	**0.50**

Table 6.15 Evaluation Process for " HRA Modeling "
(values are inserted in column-6 in table 6.16)

Results from tables 6.6 through 6.15 are imported into table 6.16 (below). "Readiness Average" is computed per each criteria. And finally the mean for "Readiness Average" for the entire list is evaluated to be at 0.82 which corresponds to Alpha-3 value.

Alpha-3: Human Factor Evaluation	***Address All Potential Scenarios***	***Comprehensive***	***Evaluation & Update***	***Effectiveness***	***Human Reliability Modeling***	***Readiness (Average)***
Safety Guidelines & EOP/AOP	0.83	1.00	1.00	1.00	0.50	0.83
Personnel Assets	0.88	1.00	1.00	1.00	0.50	0.83
Communication	0.88	0.93	1.00	1.00	0.50	0.83
Equipment Deployment Readiness	0.13	0.93	1.00	1.00	0.50	0.83
Human Reliability Analysis (HRA)	0.50	1.00	0.83	0.92	0.50	0.75
						0.82

Table 6.16 Alpha-3 Evaluation Summary

6.2.4 Alpha-4: Physical Features and Barriers in NPP Evaluation

The evaluation process for Alpha-4 is summarized in table 6.19 (below). First, a list of physical barriers is established: EE barriers, flood walls, physical islands and external water source. Second, applicable criteria is established such as robustness and reliability. Third and final step is formulating test parameters for each item listed in step two. Each test is credited as discussed in "Task/Test Parameter Credits" table 5.3 in chapter 5.

The evaluation of "Adequate, Safe and robustness " is summarized below. The weighted average is calculated in the last row and then inserted in the second column of Alpha-4 Summary table 6.19.

Adequate, Safe & Robust	**Wind, Fire, Seismic, Low temp. Barriers**	**Flood Walls Gates/Vents**	**Physical Islands**	**External Water Source**
Protect Major Component	1	0.5	0.5	1
Multi-layer Defence Approach	1	0	0.5	1
Increased Safety Factor	1	1	1	1
Meets DBEE Requirements	1	1	1	1
Computational Loading Studies	1	1	1	1
Weight Average	**1**	**0.7**	**0.8**	**1**

Table 6.17 Evaluation Process for " Adequate, Safe and robustness "
(values are inserted in column-2 in table 6.19)

The evaluation of "Reliability" criteria is summarized below. The weighted average is calculated in the last row and then inserted in the third column of Alpha-4 Summary table 6.19.

Reliability	**Wind, Fire, Seismic, Low temp. Barriers**	**Flood Walls Gates/Vents**	**Physical Islands**	**External Water Source**
Periodic Testing	0.5	0.5	0.5	0.5
Data Collection & Analysis	1	1	1	1
Continued Maintenance & Upgrade	1	1	1	1
Constant Feedback from Industry/IAEA	1	1	1	1
Weight Average	**0.875**	**0.875**	**0.875**	**0.875**

Table 6.18 Evaluation Process for " Reliability "
(values are inserted in column-3 in table 6.19)

Results from tables 6.17 through 6.18 are imported into table 6.19 (below). "Readiness Average" is computed per each criteria. And finally the mean for "Readiness Average" for the entire list is evaluated to be at 0.88 which corresponds to Alpha-4 value.

Alpha-4: Physical Barriers Evaluation	***Adequate, Safe & Robust***	***Reliability***	**Readiness (Average)**
Wind, Fire, Seismic, Low temp. Barriers	1.00	0.875	0.94
Flood Walls Gates/Vents	0.70	0.875	0.79
Physical Islands	0.80	0.875	0.84
External Water Source	1.00	0.875	0.94
			0.88

Table 6.19 Alpha-4 Evaluation Summary

6.2.5 Relative Risk Factor for Tsunami: $P_{Tsunami}$

EMP assessment model does accommodate for multiple External Events in its assessment. Typically, P_e value is obtained from the NPP DBEE report. In this example $P_{Tsunami}$ is assumed to be one (1.00 or 100%) as an illustration for single EE *EMP* assessment. Note, other EEs can be included with their respective Alpha-factors to evaluate *EMP* factor and will be discussed later.

6.2.6 *EMP* Evaluation Summary: Single EE "Tsunami"

Summary of evaluated alpha-parameters from earlier sections for Tsunami event is as follows:

EE Risk (P_e) Tsunami Event	Alpha-1 (α_1) Emergency Equipment	Alpha-2 (α_2) Safety Features	Alpha-3 (α_3) Human Reliability	Alpha-4 (α_4) Barriers
1.00	**0.70**	**0.88**	**0.82**	**0.88**

Table 6.20

Therefore, computing *EMP* factor:

EMP = $P_e[\ 1/4\ (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)_e\ ]$ (eq. 5.1)

= (1.00)*[(0.25)*(0.70 + 0.88 + 0.82 + 0.88)]

= **0.82 (or 82%)**

Consequently, NPP Vulnerability due to EE is evaluated as:

NPP Vulnerability = 1 - EMP (eq. 5.2)

= (1.00) - (0.82)

= **0.18 (or 18%)**

6.3 Case Study - 2

EMP and *NPP Vulnerability* Evaluation due to "Multiple External Events"

The EMP evaluation to multiple EE is executed in similar fashion as single EE evaluation. (1) First step is determining the required External Event (such as External Flood, External Fire, High Wind) to be included in the EMP evaluation. (2) the next step is conducting the relative risk ranking as illustrated in chapter 5.2.2. (3) the third step is assessing the alpha-factor for each corresponding EE considered in the EMP analysis, as seen in section 6.1 for single EE “Tsunami Evaluation". To illustrate the computation of a multi-external event *EMP* assessment, we will consider the following EE in the analysis: External Fire, External Flood, Snow Storm (low temperature), extreme winds and Tsunami (refer to figure 6.2 Multiple EE logic Diagram).

6.3.1 Relative Risk Factors Assessment

External events potential risks and/or probabilities are specific to each individual NPP site's geography, location and layout design and statistical data should be found within the DBEE report for the NPP. Since this information is never made public, we will assume relative risk ranking from chapter 5.2.2 as follows:

External Event	External Flood	External Fire	Extreme Wind	Snow Storm	Tsunami	Sum
External Flood	-	2x	x	3x	10x	16x
External Fire	0.5x	-	2x	3x	25x	30.5x
Extreme Wind	x	0.5x	-	2x	x	4.5x
Snow Storm	0.33x	0.33x	0.5x	-	5x	6.15x
Tsunami	0.1x	0.04x	x	0.2x	-	1.34x
					Total Sum	**58.5x**

Table 6.21 Relative Risk Ranking Method

Now, evaluating (x):

Total Sum =	**58.5 x**
58.5x = 1 (or 100%) --> x =	**0.0171**

Now, evaluating $\boldsymbol{P_e}$

EE Type	$\boldsymbol{P_e}$	(%)
External Flood	16x 16*0.0171 = 0.27	27
External Fire	30.5x 30.5*0.0171 = 0.52	52
Extreme Wind	4.5x 4.5*0.0171 = 0.08	8
Snow Storm	6.15x 6.15*0.0171 = 0.11	11
Tsunami	1.34x 1.34*0.0171 = 0.02	2

Table 6.22 Relative Risk Ranking

6.3.2 Alpha-Factors Evaluation

Step two in the *EMP* assessment of multi-EE is the evaluation of the four alpha-factors for each EE considered in the *EMP* evaluation. Evaluation process of the alpha-factor for each EE is similar to that discussed in 6.2.1 through 6.2.4 for single event "Tsunami". In the case of the Fukushima Daiichi plant accident, below is a *hypothetical* alpha-factors values summary to be used for illustration purposes only during this *EMP* computation assessment exercise:

Alpha-Factors / EE	Alpha-1 α_1	Alpha-2 α_2	Alpha-3 α_3	Alpha-4 α_4
External Flood	0.72	0.81	0.84	0.80
External Fire	0.95	0.97	0.93	0.91
Extreme Wind	0.94	0.91	0.98	0.93
Snow Storm	0.96	0.97	0.92	0.90
Tsunami	0.70	0.88	0.82	0.88

Table 6.23 Alpha factors for multiple EE

6.3.3 *EMP* Evaluation: Multiple External Events

Computing *EMP* factor:

EMP = $P_e[\ 1/4\ (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)_e\ ]$ (eq. 5.1)

= (0.27)*[(0.25)*(0.72 + 0.81 + 0.84 + 0.80)] + ... (External Flood)

(0.52)*[(0.25)*(0.95 + 0.97 + 0.93 + 0.91)] + ... (External Fire)

(0.08)*[(0.25)*(0.94 + 0.91 + 0.98 + 0.93)] + ... (Extreme Wind)

(0.11)*[(0.25)*(0.96 + 0.97 + 0.92 + 0.90)] + ... (Snow Storm)

(0.02)*[(0.25)*(0.70 + 0.88 + 0.82 + 0.88)] ..... (Tsunami)

= **0.898 (or 89.8 %)**

Consequently, NPP Vulnerability due to EE is evaluated as:

NPP Vulnerability = 1 - EMP (eq. 5.2)

= (1.00) - (0.898)

= **0.102 (or 10.2%)**

6.3.4 Multiple External Events: Logic Model Representation

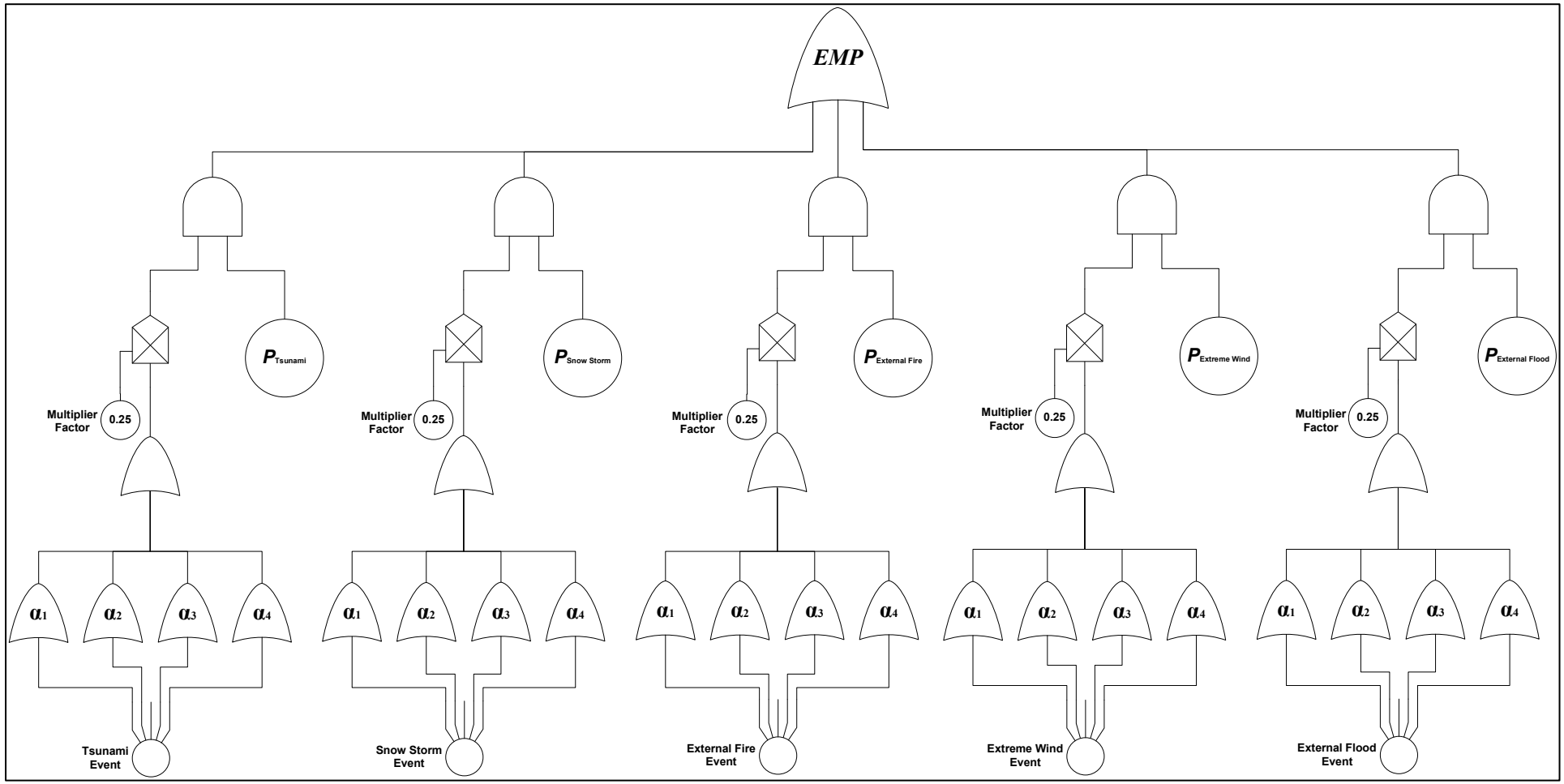

Figure 6.2 Logic Diagram for Multiple EE:
EMP Assessment

Chapter 7

7.1 *EMP* Assessment and Analysis

Case (1): Single EE "Tsunami"

The purpose of the *EMP* metric is to provide NPP a general assessment level on the plant mitigation readiness in the event of severe accidents due to EE. Below is an evaluation of the *EMP* value for a single-EE Tsunami (results used from section 6.2). The *NPP Vulnerability* is computed to be 18% indicating critical high emergency mitigation readiness in the event of a Tsunami. The alpha-factors assessment (see table 6.23) illustrates the following NPP weaknesses present in the Fukushima NPP such as:

- An Alpha-1 value of 0.7 (or 70%) shows that the Fukushima NPP lacked an adequate EME strategy for a Tsunami event and its consequences. The grid power (class IV power), EDGs power (class III power) and back-up batteries power (class II power) was lost and never restored fully during the accident to provide sufficient emergency power to operate critical component to control and contain the reactor core. The critical low assessment of alpha-1 is based on the following facts: (1) EDGs being located on-site's basement that was flooded shortly after the Tsunami hit (2) No available nearby (offsite) storage of EDGs or Batteries to power the NPP (3) Lack of deployment planning for EDGs, pumps and other EME tools and equipment. For these reason, the EME factor was assessed to be low (at 70%) which illustrates present Fukushima EME strategy for single external event (Tsunami) was not capable in restoring ultimate heat sink to the reactor core and failed to restore electric power to primary safety equipments in the NPP.

- During the evaluation of Alpha-2 value of 0.88 (or 88%), the analysis shows a low 0.67 (table 6.6) when evaluating the NPP safety features to "withstand BDEE requirements". This assessment is based the failure of (1) active safety systems (2) passive safety systems and (3) the reactor building to protect and control the reactor core as well as (4) the failure to mitigates Hydrogen gas and (5) provide continued cooling to spent fuel. The low value of 0.67 indicates key safety systems failed to provide ultimate heat sink to protect the core from damage as well as contain the reactor during BDEE. Hydrogen mitigation is essential to NPP and public safety. Unfortunately, Fukushima plant was not equipped to mitigate rapid Hydrogen production (no PARs installed and no effective SAMGs implementation to mitigates Hydrogen gas).
- The assessment of Alpha-3 value of 0.82 (or 82%) analysis shows a critical low of 0.50 (table 6.11) when evaluating Human Reliability modeling. Reason for this low credit is due to the lack of safety guidelines, EOP and AOP to manage such un-expected EE scenario. The nuclear operators/workers were not trained for such a severe accident scenario nor did they receive adequate technical support to control the reactor core more effectively. Further, poor communication, ineffective of EME deployment readiness strategy and lack of HRA analysis also contributed to the low evaluation of Alpha-3.
- An Alpha-4 value of 0.88 (or 88%) analysis shows that the NPP physical barriers components such as flood wall, gates and vents were inadequate to protect the NPP from flooding. The Fukushima NPP was flooded soon after the Tsunami event which indicates failure of physical barriers to withstand the flood and protect reactor buildings.

It is plausible to believe that if the Fukushima plant has an adequate flood wall barriers that exceeded the height of the Tsunami wave, the Fukushima accident would have had minimal, impact on the NPP and no core damage/release of radioactive materials would have been averted.

Case (2): Multi External Events

The *EMP* factor for multi-external events is computed (as seen in section 6.3) to be 0.898 (or 89.8%). Consequently, the plant *NPP Vulnerability* is valued at 0.102 or (10.2%). Table 6.23 shows the alpha-factors for External Flood and Tsunami are relatively much lower the remaining EEs. This is an indication of inadequate mitigation readiness planning for these two external events and a call to improve those areas immediately is required. Further, the two troubled mitigation readiness areas can be further investigated to show (1) that the lack of needed EME such as EDGs, pumps, tools and accessories, batteries, EME storage, EME deployment planning for both events (2) ineffective safety systems to control the core: Isolation Condensers were not fully employed, other safety system were either not available or un-functional (3) inadequate physical barrier to protect the NPP site and main buildings: insufficient sea wall height to protect against high waves, flood doors to withstand waves' pressure and keep water out (4) operators lack of experience and training to deal with severe accidents and the lack of expert support to control effectively the reactor core temperature and mitigate radiation release from the primary containment. The EMP analysis should be imported into the NPP safety design and emergency mitigation readiness planning to minimize EE potential impact on the NPP.

7.2 Conclusion

The Fukushima accident was a wakeup call for the industry to address in-depth (1) Beyond Design Basis Events BDBE and (2) emergency mitigation for multi unit failure scenarios. The Fukushima accident highlighted the need for serious emergency mitigation planning against EE that is adequate and effective. There are many lessons learned from Fukushima such as the need to (1) have adequate EE mitigation planning (2) improve active and passive safety systems (3) increase human reliability and corporate safety culture to face severe accident scenarios (4) investment in physical barriers to protect NPP site; all the above lessons are captured by the *EMP* assessment model.

Current symptom-based approach to mitigates accidents relying only on onsite defense in depth strategy proved incapable - in the case of Fukushima - to control, contain and cool the reactor. The EMP model illustrated relying on nuclear site's multiple layers of emergency equipment is a mere subset of a bigger and more comprehensive approach to provide ultimate control/containment of the reactor and to provide higher safety assurances to workers and surrounding community during severe accidents. During the EMP evaluation process, it was revealed the gaps and potential opportunities to improve with regards to emergency mitigation readiness and consequent issues related to NPP vulnerability due to BDBEs. Thus making EMP a great metric tool to optimize NPP emergency mitigation planning and minimize potential NPP vulnerability due to BDBE/external events. Further, EMP model can be used as an important feedback mechanism to improve NPP emergency and safety compliance.

7.3 Recommendations and Future Work

Emergency Preparedness (EP) is an integral safety function in NPPs. Unfortunately EP continues to lack behind, despite advancements in nuclear power, and continue to catch up only when serious accidents (such as Three Mile Island or Fukushima) take place. This paper recommends:

- Refinement of the EMP model to distinguish the alpha factors values and address the time dependency for deployment of EME.
- A shift in NPP emergency response from being a symptom-based approach to a defense by design approach. The future of NPP must capitalize on advancement in nuclear technology, a better NPP structural design, and reliance on artificial intelligence. The current NPP design can sustain SBO for a limited time period (measured in hours) due to limited heat sink available. Also human intervention is required with procedure such as EOP/AOP/SAMG to be implemented in a time sensitive manner; otherwise, SOB and consequently the loss of ultimate heat sink are considered a major NPP Vulnerability that may lead to a nuclear disaster similar to those of Three Mile Island and Fukushima. The future NPP must be able to sustain loss of SBO by relying on more advance passive and natural head sink systems for days without human intervention by relying on better reactor design, application of (thermal) natural forces for cooling and application advance monitoring and computing equipment
- The current primary driver to produce clean electricity power is not enough. The driver should be to produce clean electricity power *safely*. In other works, the safety should be the main design criteria. The Three Mile Island and Fukushima accidents are evidently preventable has safety been applied. NPP must find a way to gauge safety in NPP for monitoring and feedback. The proposed EMP model and assessment is a good start but a more comprehensive research in this area is required by the nuclear operators and nuclear industry regulators.

References

References:

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants No. NS-G-1.5, IAEA, Vienna (2003).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design No. SSR-2/1, IAEA, Vienna (2012).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Flood Hazards for Nuclear Power Plants on Coastal and River Sites, Safety Standards Series No. NS-G-3.5, IAEA, Vienna (2003).

[4] National Oceanic and Atmospheric Administration (NOAA), Ocean Facts, retrieved from: http://oceanservice.noaa.gov/facts/cyclone.html. (August, 2013)

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological Events in Site Evaluation for Nuclear Power Plants, Safety Standards Series No. NS-G-3.4, IAEA, Vienna (2003).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, Safety Standards Series, IAEA, Vienna.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Emergency Power Systems in Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (in preparation).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).

[9] Ericson, C. (1999). Fault Tree Analysis - A History. *17th International System SafetyConference .* Seattle: The Boeing Company.

[10] Mosleh, A., Fleming, K., Parry, G., Paula, H., Worlede, D., & Rasmuson, D. (1989). *Procedures for Treating Common Cause Failures in Safety and Reliability Studies.* Palo Alto: EPRI.

[11] Hirschberg, S., Parry, G. W., & Carlsson, L. (1992). *Procedures for conducting common cause failure analysis in probabilistic safety assessment.* Vienna: IAEA.

[12] Kancev, D., & Cepin, M. (2012). Limitation of Explicit Modeling of Common Cause Failures within Fault Trees. *IEEE*.

[13] Vrbanic, I., Kosutic, I., Vukovic, I., & Simic, Z. (2003). Presentation of Common Cause Failures in Fault Tree Structure of Krsko PSA: An Historical Overview. *International Conference Nuclear Energy for New Europe 2003.* Slovenia.

[14] Fleming, K., Rao, S., Tinsley, G., Mosleh, A., & Afzali, A. (1992). *A Database of Common-Cause Events for Risk and Reliability Applications.* Palo Alto: EPRI.

[15 U.S.NRC, INPO. *The United States of America National Report for the 2012 Convention on Nuclear Safety Extraordinary Meeting - NUREG-1650*. Washington D.C.: U.S.NRC, 2012.

[16 Mitigation of Hydrogen Hazards in Severe Accidents in Nuclear Power Plants (IAEA-TECDOC-1661). Vienna: IAEA, 2011.

[17] Canadian Nuclear Safety Commission . *Emergency Management and Fire Protection: Nuclear Emergency Preparedness and Response*. Ottawa: CNSC, 2013.

[18] U.S.NRC. *Issuance of Order to Modify Licenses with Regard to Requirements for Mitigation Strategies for Beyond Design Basis External Events*. Washington: U.S.NRC, 2012.

[19] National Disaster Management Authority Government of India. *National Disaster Management Guidelines - Management of Nuclear and Radiological Emergencies*. New Delhi: National Disaster Management Authority Government of India, 2009.

[20] Ontario Ministry of Community Safety and Correctional Services. Provincial Nuclear Emergency Response Plan. 17 10 2013 <http://www.emergencymanagementontario.ca/english/emcommunity/response_resources/plans/provincial_nuclear_emergency_response_plan.html>.

[21] Nuclear Energy Institute. *Diverse And Flexible Coping Strategies (FLEX) Implementation Guide*. Washington D.C.: Nuclear Energy Institute, 2012.

[22] World Association of Nuclear Operators - WANO.

<http://www.wano.info/en-gb/library/documentslibrary>

[23] Canadian Nuclear Safety Commission. *CNSC Staff Action Plan on the CNSC Fukushima Task Force Recommendations INFO-0828.*

< http://www.nuclearsafety.gc.ca/pubs_catalogue/uploads/INFO-0828-Draft-CNSC-Staff-Action-Plan-on-Fukushima-Dec-2011_e.PDF>

Appendices

Appendix A: External Flood

System Affected	Potential Damage	Recommendations
▪ **Building Structures** ▪ **Outside equipment** ▪ **Ventilation System** ▪ **Air Supply** ▪ **Diesel Generators** ▪ **Pump Houses** ▪ **Site Accessibility** ▪ **Cooling Tower** ▪ **Trained personnel** ▪ **Site Accessibility (land and off shore)**	▪ Inundation of site Structures ▪ Inundation of key equipment ▪ Damage of Safety Equipment ▪ loss access to Outdoor Equipment ▪ Loss of safety function ▪ loss of Air Intake ▪ Loss of AC Power ▪ Loss of Emergency Power (from diesel) ▪ limited or no availability of service water due to loss of power ▪ Damage to cooling tower ▪ Flooding of pump houses ▪ Site roads ▪ Reactivity Control ▪ Confinement System ▪ Loss of UHS ▪ Access to NPP by trained personnel ▪ Infrastructure damage to in and around the NPP site	▪ Construction of external barriers, natural or artificial islands ▪ Active and passive barriers should be incorporated in the site structures directly (retaining walls, penetration closures) ▪ Improve drainage system reliability and functionality and increase their safety margin to withstand heavy precipitation. ▪ Implement Active and passive drainage system in site design and ensure they are adequate for site specific. (i.e. automatic flood gate and vent shaft system) ▪ Improve sealing in structural joints or cable conduits and inspection opening, to limit in-leakage into site structures. ▪ Identify floods causes for each plant site and place operational procedures such that real time monitoring data for the flood causes are tracked. This will enable the NPP to have a warning system to shut down the reactor core safely in the event of potential flooding. ▪ Design all safety systems including warning systems to withstand flood, and flood secondary events such as high wind and landslide. ▪ Structures should withstand both static and dynamic forces of floods (such as effects of ice, water, debris carried by flood and waves) ▪ Site design must deal with secondary flood effect: sedimentation, modification of water salinity, erosion, blockage of intakes (by ice or debris) and mud suspension in water ▪ Emergency power supply plane should be in place in event of loss of AC power and the onsite diesel generator power. ▪ Loss of cooling tower: alternatively a different method of providing cooling water to the plant could be provided, for example from a different source or by a closed loop air cooled system. ▪ real time monitoring of flood causes and establishing warning system

Appendix B: External Fire

System Affected	Potential Damage	Recommendations
▪ **Building Structures** ▪ **Outside (i.e. electrical) equipment** ▪ **Ventilation System** ▪ **Air Supply** ▪ **Diesel Generators** ▪ **Site Accessibility** ▪ **Visibility (land and off shore)**	▪ Structures integrity ▪ Safety Equipment ▪ Outdoor Equipment ▪ Loss of safety function (including operator action) ▪ Air Intake ▪ Loss of AC Power ▪ Loss of Emergency Power (from diesel) ▪ limited or no availability of service water due to loss of power ▪ Site roads blockage ▪ Infrastructure damage to in and around the NPP site ▪ Reduce visibility and site accessibility	▪ Eliminates combustibles and proper protection of combustibles around site ▪ Develop physical barriers and zones to contain fire ▪ Remove propagating medium (i.e. remove trees/vegetation near site) ▪ Ensure durable site structure to withstand fire heat flux (determine max heat flux: capacity of concrete to absorb thermal load is determined by structure features such as thickness and composition of aggregate material). If inherit heat capacity of NPP structure is not sufficient, then increase concrete thickness of the exposed structure. ▪ Steel structure is not suitable for fire protection; thus it should not be part of defence in depth for External fire analysis. However, steel is a good safety defence for protection against air craft/induced wind missiles) ▪ General fire protection (equipment/personnel/training/command) ▪ Ventilation system should be designed to prevent smoke and heat from affecting safety systems. Protection of ventilation systems by isolation of the systems from outside air by means of dampers. Also, there should be a separation of the inlet and exhaust hoods of one ventilation system serving one safety system/area from another inlet/exhaust hood serving a second system/area. ▪ Adherence to building code and material guidelines to protect against fire ▪ In depth defences against fire should incorporate redundant safety systems, physical separation by distance, by fire compartment, by specific barriers. ▪ Protection of air intake for diesel generators by separation by distance. ▪ Ability to clear roads and off-shore access by heavy equipment if necessary ▪ Emergency power supply plane should be in place in event of loss of AC power and the onsite diesel generator power. ▪ Multiple and better Fire detection and extinguishing systems to ensure a safe shutdown manner. ▪ Control room my function without ventilation system for 4-6 hrs. Emergency planning should be in place to provide adequate clean air in order to operate safety equipment. Establish early warning system and safety procedures

Appendix C: Extreme Wind

System Affected	Potential Damage	Recommendations
▪ **Building Structures** ▪ **Outside equipment** ▪ **Diesel Generators** ▪ **Cooling Towers** ▪ **AC power** ▪ **Emergency Power** ▪ **Ventilation System** ▪ **Instrumentation Control** ▪ **Ultimate Heat System (UHS)** ▪ **Site Access Roads (land and off shore)**	▪ Safety Equipment ▪ Structure integrity ▪ Outdoor Equipment (i.e. cranes, electrical) ▪ Loss of off-power ▪ Loss of Emergency Power (from diesel) ▪ Affect ventilation system ▪ Creates false signals to instrumentation due to pressure differentials ▪ Corrosion and malfunction of electrical equipment due to salt spray ▪ collapse of cooling tower ▪ UHS damage could prevent the transport and absorption of residual heat ▪ limited availability of service water due to loss of power ▪ Site roads blockage ▪ Site roads blockage ▪ Infrastructure damage to the NPP site	▪ Extreme winds carrying moisture may cause flooding. Protection against such must be exercised (see above) ▪ NPP may be exposed to salt sprays from the sea in the form of a precipitation which will damage exposed electrical equipment and cause corrosion and malfunction. Protection of exposed system is required. ▪ Ensure no significant water level change is the system that might affect UHS functions ▪ Ability to clear roads and off-shore access by heavy equipment if necessary ▪ Protection of cooling tower from air born objects, if possible ▪ Erection of physical barriers to protect site structure, water intakes and UHS structures from damaged caused object (ship) missiles collision, ice or floating debris. ▪ Establish early warning system and safety procedures

Appendix D: Extreme Low Temperature / Snow Storm

System Affected	Potential Damage	Recommendations
▪ **UHS** ▪ **AC Power** ▪ **Emergency Power** ▪ **Safety Equipment** ▪ **Ventilation System** ▪ **Building Structures** ▪ **Pump houses** ▪ **Cooling Towers** ▪ **Site accessibility**	▪ Availability of UHS system ▪ Availability of site power ▪ I&C equipment malfunction (due to moisture, lightning, low temperature) ▪ Low temp. may cause ventilation system to malfunction ▪ Moisture condensation in sensitive and safety equipment and I&C due to low temperature ▪ Ice damage of ventilation air intake and discharges ▪ Ventilation shafts could not be closed ▪ freezing pipe & ruptures ▪ Water damage in I&C room at lower elevations ▪ Ice can cause excess loading on site structures	▪ Intake structures for the heat transport systems should be designed to provide an adequate flow of cooling water during seasonal water level fluctuation. ▪ Due allowance should be made for the effects of extreme cold weather conditions on make-up supplies ▪ Ensure UHS design is capable and functional in these events by testing and analysis. This would include the monitoring the operability of spray nozzles to check that they do not become frozen or intake screens blocked by ice. ▪ Alternative path(s) for water cooling should be provided to counter the formation of frazil ice at the service water intake. In this case, provision should be made for adequate instrumentation and alarms and relevant procedures and training. ▪ Protection from ice blocks and floating debris that could damage water intakes and pump houses

	▪ Snow induced damage on electric grid and availability of power ▪ Access by the operator to external safety related facilities and mobility of emergency vehicles is limited ▪ flooding/malfunction of pump houses ▪ Access to NPP by trained personnel ▪ Access to facilities within the NPP site ▪ Site roads blockage Infrastructure damage to in and around the NPP site	