

Identification and Documentation of Environmental
Assumptions for the PACEMAKER System

IDENTIFICATION AND DOCUMENTATION OF
ENVIRONMENTAL ASSUMPTIONS FOR THE PACEMAKER
SYSTEM

BY
VIVIEN WANG, B.Eng.

A THESIS
SUBMITTED TO THE DEPARTMENT OF COMPUTING AND SOFTWARE
AND THE SCHOOL OF GRADUATE STUDIES
OF MCMASTER UNIVERSITY
IN PARTIAL FULFILMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF APPLIED SCIENCE

© Copyright by Vivien Wang, March 2012

All Rights Reserved

Master of Applied Science (2012)
(Computing and Software)

McMaster University
Hamilton, Ontario, Canada

TITLE: Identification and Documentation of Environmental Assumptions for the PACEMAKER System

AUTHOR: Vivien Wang
B.Eng., (Software Engineering)
McMaster University, Hamilton, Canada

SUPERVISORS: Drs. Douglas Down, Alan Wassying

NUMBER OF PAGES: ix, 201

Abstract

An interest has been established in the identification, documentation and classification of the environmental assumptions that are missing from the original *PACEMAKER System Specification*. This thesis addresses the presented challenge and documents the procedure used to identify, classify, and document these missing environmental assumptions.

In summary, this thesis answers the following questions:

1. What can be done in order to improve the original *PACEMAKER System Specification* with respect to environmental assumptions?
2. Why is it beneficial, in terms of enhancing software quality, to include the documentation of environmental assumptions – which sometimes are (wrongfully) perceived as being collateral and optional – as part of the software requirements document?
3. How should such environmental assumptions be documented?

More specifically, this thesis

- Presents an abstract model for the PACEMAKER system.
- Identifies system boundaries and interfaces in the PACEMAKER model.
- Identifies environmental assumptions for the PACEMAKER system.

- Presents a classification system for the environmental assumptions identified for the PACEMAKER system based on the proposed model.
- Proposes a process for identifying environmental assumptions.

Furthermore, the research findings presented in this thesis are not limited to the PACEMAKER system. The documentation convention proposed in this thesis is meant to be generalized and can be extended to address similar documentation needs posed by all kinds of software systems. Additionally, the process of environmental assumptions elicitation described in this thesis provides a useful reference for conducting similar assumption identification projects. Lastly, the classification system presented in this thesis for the environmental assumptions exhibits one facet of a grander conceptual system – one that incorporates multiple ‘*views*’ of the same set of assumptions, with each *view* being distinguished by a unique set of classification criteria.

Acknowledgements

I would like to thank Dr. Down Dr. Wassying, and my loving family..

Contents

I	INTRODUCTION	1
1	Introduction	2
1.1	Motivation – the Pacemaker Formal Methods Challenge	2
1.1.1	Introduction to the Challenge	2
1.1.2	The PACEMAKER System Specification	2
1.2	Research Problem and Scope	3
1.3	Contribution of this Thesis	3
II	Artificial Cardiac Pacemaker as a Medical Instrumentation System – from the generic to the specific	6
2	First Principles of Medical Instrumentation	7
2.1	Anatomy and Physiology	8
2.2	Physiological Systems of the Body	9
2.3	Biomedical Signals, Bioelectric Signals, and Biopotential Electrodes .	10
2.4	Biomedical Telemetry	16

2.5	Basic Medical Instrumentation System	17
2.6	General Constraints in Design of Medical Instrumentation Systems	22
2.7	Regulation of Medical Devices	28
2.7.1	Standards	30
2.7.2	Regulatory Requirements	31
2.7.3	Standards Related Agencies	33
3	Artificial Cardiac Pacemaker as a Medical System	35
3.1	Anatomy of the Heart	36
3.2	The Electrophysiology of the heart	37
3.2.1	The Electrical Conduction System of the Heart	39
3.2.2	The Pacemaker Site	41
3.2.3	Requirements for Effective Pumping	42
3.3	The Cardiac Cycle	44
3.4	The ECG: Recording Heart Activity	45
3.4.1	Heart Electrical Forces	45
3.4.2	ECG Waves and Intervals	46
3.5	Pacemaker Indications and Contraindications	50
4	Operational Characteristics of an Artificial Pacemaker	51
4.1	Terminology and Basic Concepts	52
4.2	Types of Implantable Pacemakers	53
4.3	Programmable Pacemaker	58
4.4	The Output Pulse of the Pacemaker	61

4.5	Operational Characteristics of a simple DDD pacemaker	62
4.5.1	Ventricular Channel	62
4.5.2	DDD pacing or VVI pacing with an atrial channel	63
4.5.3	Derived timing cycles	63
4.5.4	Atrial refractory period	63
4.5.5	<i>Upper rate interval</i> vs. PVARP as a basic interval	64
4.5.6	The six intervals of a simple DDD pacemaker	64
4.5.7	The fifth fundamental timing cycle	65
4.5.8	VSP and Upper Rate Interval programmable independently of the TARP	65

III Identification and Documentation of Environmental Assumptions for the PACEMAKER System 67

5 Modeling the PACEMAKER System 68

5.1	Definitions and Concepts	69
5.2	A Formal Model for the PACEMAKER System	70
5.2.1	The Four-Variable Model	70
5.2.2	Modeling the PACEMAKER System	74
5.2.3	The Domain Environment and Sub-environments	75
5.2.4	The PACEMAKER Model – System Boundaries and Interfaces	80

6 Environmental Assumptions at System Boundary B1.1 for the PACEMAKER Model 88

6.1	Identifying Environmental Assumptions Concerning System Boundary	
1.1:	Heart \longleftrightarrow Complete System	90
6.2	Refinement of the Elicited Environmental Assumptions	91
6.2.1	The Type of Assumptions	92
6.2.2	Classification and Organization of the Assumptions – Docu- mentation Convention	94
6.3	Aspects of NAT governed by the Cardiovascular System	95
6.3.1	Characteristics of the Biosignal	95
6.3.2	Characteristics of Natural Cardiac Pacemakers	98
6.3.3	Interference among Physiological Systems	100
6.3.4	Safe Levels of Applied Energy	101
6.4	Assumptions Concerning Ventricular/Atrial Stimulation	104
6.4.1	Assumptions concerning refractory periods	104
7	Assumptions on System Hardware (B2)	108
7.1	An Extension to the Proposed Documentation Convention	109
7.1.1	Likelihood of Change Index	110
7.2	Environmental Assumptions Concerning the Leads	111
7.2.1	Assumptions Concerning Bipolar Leads	112
7.2.2	Assumptions Concerning the Sensing Electrode Impedance . .	114
7.3	Environmental Assumptions Concerning the System Hardware Archi- tecture of the PACEMAKER System	115
7.3.1	System Architecture	115

7.4	Environmental Assumptions Concerning the Sensing Circuit: the Band-Pass Filter, the Threshold Detector, and the Amplifier	120
7.4.1	General	120
7.4.2	Band-Pass Filter:	121
7.4.3	Amplifier and Threshold Detector	122
7.5	Environmental Assumptions Concerning the Output Circuit	124
7.6	Environmental Assumptions Concerning the Timer/Timing Control Circuit	126
7.7	Environmental Assumptions Concerning the Battery	128
8	Assumptions Concerning (Software) System Behaviour	133
8.1	Another Extension to the Proposed Documentation Convention . . .	135
8.2	Timing Cycles In The Eyes Of The Software	136
8.2.1	Lower Rate Limit/Interval (LRI)	136
8.2.2	Pacemaker Ventricular Refractory Period (VRP)	137
8.2.3	Atrioventricular Interval (AVI)	140
8.2.4	Atrial Refractory Period	143
8.2.5	Postventricular Atrial Refractory Period (PVARP)	144
8.2.6	Blanking Periods	146
8.2.7	Upper Rate Interval (URI)	153
8.2.8	Ventricular Safety Pacing Window (VSP)	154
8.2.9	Atrial Escape Interval (AEI)	157
8.2.10	Total Atrial Refractory Period (TARP)	158
8.3	Influence of Events in One Chamber upon the Other	160

8.3.1	Atrial Channel	160
8.3.2	Ventricular Channel	161
9	Other Environmental Assumptions Concerning System Boundaries	
	B1.2 and B1.4	164
9.1	Further Extension to the Proposed Documentation Convention	165
9.2	Environmental Assumptions Concerning System Boundary B1.2 – the Magnet Interface	166
9.3	Environmental Assumptions Concerning System Boundary B1.4 – the Serial Communication Interface	169
10	Lessons Learned from the Identification and Documentation of En- vironmental Assumptions in the PACEMAKER Project	176
10.1	Lesson 1: Domain investigation – Identify the search space for envi- ronmental assumptions, start with the most generic	178
10.2	Lesson 2: Prune the search space by studying the characteristics and constraints present in current mainstream artificial pacemakers	179
10.3	Lesson 3: Study the domain environment extensively and understand the critical requirements posed by the encompassing environment on the control system	180
10.4	Lesson 4: Thoroughly understand the device or control system under consideration	181
10.5	Lesson 5: Model the system	182
10.6	Lesson 6: Identify system boundaries and interfaces	183

10.7 Lesson 7: Elicit environmental assumptions at each system bound- ary/interface	184
10.8 Lesson 8: Refine environmental assumptions at each level of specificity	185
10.9 Lesson 9: Classify the environmental assumptions	186
10.10 Lesson 10: Develop a documentation convention and use it consistently	188
10.11 Lesson 11: Allow extension and flexibility of the documentation con- vention	188
11 Conclusion and Future Work	192
11.1 Conclusion	192
11.2 Future Work	194
11.2.1 Provide different ‘views’ in rendering the documented assump- tions	194
11.2.2 Index of Likelihood of Change	195
A Acronyms	196

List of Figures

2.1	A. Schematic view of an idealized action potential illustrates its various phases as the action potential passes a point on a cell membrane. B. Actual recordings of action potentials are often distorted compared to the schematic view because of variations in electrophysiological techniques used to make the recording. [24]	13
2.2	A basic medical instrumentation system as a control system.	19
3.3	Interior anatomy of the human heart [5].	38
3.4	Structure of the implantable part of a pacemaker system, and its arrangement inside a patient's body.	39
3.5	The Electrical Conduction System of the heart. (<i>Image adapted from [8]</i>)	40
3.6	Schematic representation of normal ECG [1]	46
3.7	Electrocardiogram wave patterns produced by electrical activity in the heart. (<i>Image adapted from [8]</i>)	48
4.8	Various pacing modes in demand pacemakers and their corresponding NASPE/BPEG codes. [<i>image adapted from [2]</i>]	57
4.9	The output pulse of the pacemaker.	61

5.10	The Modified Four Variable Model with Hardware Hiding [23]	71
5.11	Proposed System Structure and System Boundaries	78
5.12	A Functional Block Diagram of the Programming Interface between PG and the Control Unit [16]	82
7.13	Block diagram of a multi-programmable pulse generator.	117
7.14	The filtering of sensed signals.	123
9.15	Functional block diagram of the magnetic communication interface. .	172

Part I

INTRODUCTION

Chapter 1

Introduction

1.1 Motivation – the Pacemaker Formal Methods Challenge

1.1.1 Introduction to the Challenge

Boston Scientific has released into the public domain the system specification for a previous generation pacemaker. A major reason for publishing this specification is to have it serve as the basis for a challenge to the formal methods community, in the spirit of other Grand Challenges [20].

1.1.2 The PACEMAKER System Specification

The complete system specification for the PACEMAKER system can be found in Appendix B.

1.2 Research Problem and Scope

This thesis defines a problem that focuses on a particular aspect of the Grand Challenge. An interest has been established in the identification, documentation and classification of the environmental assumptions that are missing from the original *PACEMAKER System Specification*. In addition, this thesis adopts a top-down approach in the research of the knowledge domain (where most of the environmental assumptions reside), exploring the properties and characteristics of the medical and biological domains of interest.

1.3 Contribution of this Thesis

In response to the PACEMAKER Grand Challenge, this thesis answers the following questions:

1. What can be done in order to improve the original *PACEMAKER System Specification* with respect to environmental assumptions?
2. Why is it beneficial, in terms of enhancing software quality, to include the documentation of environmental assumptions – which sometimes are (wrongfully) perceived as being collateral and optional – as part of the software requirements document?
3. How should such environmental assumptions be documented?

However, the contribution of this thesis is not limited to its application on a specific medical device, namely the PACEMAKER system. For starters, the convention and documentation approach proposed in this thesis for the PACEMAKER system's environmental assumptions are meant to be generalized and used to address similar documentation needs posed by all kinds of software systems. Additionally, the process of environmental assumptions elicitation described in this thesis provides a useful reference for conducting similar assumption identification projects. Lastly, the classification system presented in this thesis for the environmental assumptions exhibits one facet of a grander conceptual system – one that incorporates multiple ‘*views*’ of the same set of assumptions, with each *view* being distinguished by a unique set of classification criteria.

Therefore, in essence, the PACEMAKER project is merely a magnified case study, demonstrating the practicality of the documentation approaches that are proposed in this thesis, and the way that they can be applied to a real-world problem to ultimately improve the quality of the software.

In summary, at the heart of this thesis are the following issues concerning environmental assumptions:

1. Their *identification* (including modeling of the system and identification of system boundaries).
2. Their *classification*.
3. Their *documentation*.

In addition to the contributions listed above, this thesis also presents comprehensive research on the related knowledge domain.

Part II

Artificial Cardiac Pacemaker as a Medical Instrumentation System – from the generic to the specific

Chapter 2

First Principles of Medical Instrumentation

If we were in an Object-Oriented world, we would think of the class *PacemakerSystem* as a child/subclass of a more general category, or a superclass in this case, the *MedicalInstrumentSystem* class. Indeed, as this implied inheritance is suggesting, the behaviour and characteristics of a pacemaker system are nothing but an extension and specialization of that of a generic medical instrumentation system. Therefore, an overview of the first principles involved in a medical instrumentation system would provide great insights into determining and specifying the behaviour of pacemaker systems.

Furthermore, there exists a set of general design constraints and government regulations that are applicable to all commercial medical instrumentation systems. It is the responsibility of pacemaker system engineers to comply with these restrictions

and specifications, which include:

- General constraints in the design of medical instrumentation systems
- Performance requirements of medical instrumentation systems
- Regulation of Medical Devices

This chapter outlines some of the essential components that form a basic medical instrumentation system, as well as the interface between the medical device and its biological environment. Components are described in their generic form, and are selected with the intention of mapping them to the corresponding parts in a pacemaker system (featured in the next chapter).

2.1 Anatomy and Physiology

“Anatomy” and “Physiology”, explained in the shortest forms, mean “structure” and “function”, respectively. In the realm of medical instrumentation system design, anatomy is the science dealing with the bodily structure of humans; physiology, on the other hand, is concerned with the normal functions of the human body and its parts.

The hallmark that distinguishes a medical instrumentation system from any other embedded system is the existence and inclusion of a *biological element*, upon which the hardware component of the system operates. With this extension in the system scope, the specification and design process of a medical instrumentation system is greatly influenced – in that, it now requires, and is highly dependent upon, knowledge

of the structure and function (or anatomy and physiology) of the particular biological component.

However, with the above said, the actual system specification produced when such a traditional design process is applied often excludes the description of the biological element of interest. Instead, it is predominantly a popular assumption in industry that the design engineers of a particular medical instrumentation system are also domain experts in the related medical field. The communication overhead between the specification writers and implementers of such medical systems is thus omitted as a result of this implicit assumption.

The purpose of this thesis is to investigate these missing environmental assumptions in the case of an artificial pacemaker system, and to develop a formal documentation methodology for these environmental assumptions, along with specifications for other functional behaviour of the system.

A formal definition of *environmental assumption* is presented in Chapter 6; and an in-depth discussion of it forms the theme of **Part IV** of this thesis.

2.2 Physiological Systems of the Body

Similar to the way a control system functions in the physical world, the human body renders itself as a multivariable-control system with numerous intricate and interacting communication networks. These physiological systems communicate internally, as well as with an external environment, in protocols that are either intrinsic to the

biological network itself or explicitly specified for conveying information to an external environment – which could just as well be any type of medical instrumentation system. These '*protocols*', manifesting themselves in the form of various *biomedical signals*, are of special importance to the design of a medical instrumentation system, as these are primarily the input to the computer-controlled medical device.

The physiological system that is central to this thesis is the ***Cardiovascular System***, which is discussed in the next chapter, where the concept of a general medical instrumentation system is instantiated into a specific reference to the artificial pacemaker system.

2.3 Biomedical Signals, Bioelectric Signals, and Biopotential Electrodes

Biomedical signals are *signals* (information/instruction-bearing media or mechanisms), which are intrinsic to a biological system and are used primarily for extracting information on the biological system under investigation by an external party. Biomedical signals originate from a variety of sources. Depending upon their source, biomedical signals can be classified into different categories, including [3, 16]:

- Bioelectric signals
- Bioacoustic signals
- Biochemical signals
- Biomechanical signals

- Biomagnetic signals
- Bio-optical signals
- Bio-impedance signals

For the purpose of this thesis' intended investigation on the pacemaker system, the contents of this thesis will restrict itself to bioelectric signals.

Bioelectric Signals

Bioelectric signals are probably the most important biosignals, due to the fact that most crucial physiological systems within the human body use bioelectric signals as their means of communication. Because bioelectric signals, as all other signals, encapsulate valuable information about their native bio- or physiological systems, it is a common practice in the medical field to use biosignals to study and monitor the main functions of the underlying physiological system. Also owing to this information-rich property of biosignals, medical devices are designed to *monitor*, *measure*, and sometimes *interfere* with the innate biosignals, in hopes of providing diagnostic or therapeutic treatment to the potentially malfunctioning body part under examination.

The bioelectric signal is unique to biomedical systems [3]. It is generated by neurons (nerve cells) and muscle cells, such as cardiac muscle cells. Its source is the potential difference existing across the cell membrane. Once the cell membrane *depolarizes* sufficiently, i.e., the membrane potential exceeds a certain threshold, it initiates an *action potential*, which is a pulse-like wave of voltage that travels along

the cell membranes. After this rapid rise, the membrane voltage is restored to its resting value. The passage of an action potential inhibits another action potential at the same spot: such an axon (or nerve fibre) is said to be ***refractory***. Figure 2.1 illustrates the idea of an *action potential*.

Because they are able to transmit information so fast, the flow of action potentials is a very efficient form of data transmission.

The electric field generated by the action of many cells constitutes the bioelectric signal [16]. A bioelectric signal can be measured using surface electrodes as sensors.

Biopotential Electrodes

Electrode, or *biopotential electrode*, is a type of *biomedical sensor/transducer*. Sensors, or transducers, convert signals of one type quantity into an equivalent signal quantity. Biomedical sensors take signals representing biomedical variables and convert them into what is usually an electrical signal [3]. As such, the biomedical sensor acts as the *interface* between two interacting systems – the intrinsic physiological system and an external electronic system.

When designing a medical instrumentation system as an embedded system, the hardware-software co-design paradigm requires the consideration of the following list of factors for the design choices made for a particular sensor [16]:

- The magnitude of quantity to be measured
- The order of accuracy required
- The static or dynamic character of the process to be studied

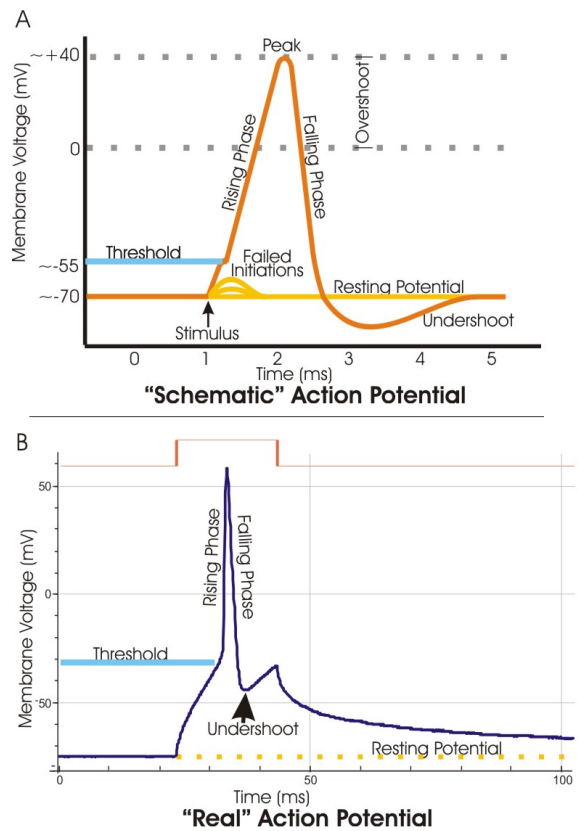


Figure 2.1: **A.** Schematic view of an idealized action potential illustrates its various phases as the action potential passes a point on a cell membrane. **B.** Actual recordings of action potentials are often distorted compared to the schematic view because of variations in electrophysiological techniques used to make the recording. [24]

- The site of application on the patient's body, both for short-term and long-term monitoring
- Economic considerations

Performance Characteristics of Sensors

A sensor is normally placed within the enclosing measured physiological system as an indwelling component; it serves as a data-collector, feeding the corresponding electronic system with input data. The performance characteristics of the sensor thereby critically determine the overall performance of the system. The performance characteristics that are deemed important for the purpose of this thesis are listed below (as a subset of a more complete list given in [16]):

- **Accuracy:** This term describes the algebraic difference between the indicated value and the true or theoretical value of the measurand. In practice, accuracy is usually expressed as a percentage of full scale output or percent of reading or \pm number of digits for digital readouts.
- **Sensitivity:** The *transfer ratio*¹ of output to input.
- **Threshold:** The threshold of the sensor is the smallest change in value of the measurand that will trigger a sensor output. It sets a lower limit on the measurement capability of a sensor.
- **Noise:** This is an unwanted signal at the output due either to internal or external sources.

¹Transfer ratio = output / input

- **Hysteresis:** Hysteresis describes the change in output with the same value of input but with a different input history. For example: hysteresis is observed when the input/output characteristics for a sensor are different for increasing inputs than for decreasing inputs. It results when some of the energy applied for increasing inputs is not recovered when the input decreases.
- **Span:** The total operating range of the sensor.

Practical Electrodes for Cardiac Signal Measurements

Because of this thesis' prevailing interest in the cardiovascular system, bioelectric signals originating inside the heart are listed in Table 2.1, along with their recording mechanisms. Table 2.1 is intended to provide an overview of the characteristics, detection and recording mechanisms of bioelectric signals related to the cardiac system, thereby laying a foundation for an in-depth discussion on these topics in the later chapters.

Table 2.1: Selected signals from Cardiovascular system

<i>Parameter</i>	<i>Primary biosignal characteristics</i>	<i>Sensor required</i>	<i>Primary converted electrical signal characteristics</i>	<i>Biological source</i>	<i>Recording mechanism</i>
Heart rate	Rate: 25–300 beats per minute. Normal human heart rate at rest: 60–90 beats/min.	Skin (surface) electrodes	Frequency range: 0.05–120 Hz, Signal amplitude: 0.1–5 μV , typical signal: 1 μV	Heart—as seen from body surface	Electrocardiogram (ECG)
		Implanted (contact) electrodes		Heart—as seen from within	Cardiac electrogram (CEG)

2.4 Biomedical Telemetry

Medical instrumentation systems, by their implantable nature, usually have system components situated in a working habitat that is inside the human body. The component that resides inside the living body is integrated with the internal physiological system via sensors and actuators, interacting with its biological environment in a bi-directional way. The implantable portion of a medical instrumentation system is essentially a mini-electronic device, controlled by microprocessors. Therefore, in order to program the device to function properly inside a patient's body in a non-invasive way, a form of communication and data transfer between the implanted component and its controller – residing outside the patient's body – has to be allowed. This channel of communication is known as the *biomedical telemetry*, whose

specification should be included as part of the complete system specification of the medical device.

Wireless Telemetry

Wireless telemetry permits examination of physiological data under normal conditions and in natural surroundings without any discomfort or obstruction to the person under investigation [16]. Two kinds of modulation systems are used in wireless telemetry – *frequency modulation* and *pulse width modulation*.

2.5 Basic Medical Instrumentation System

A component-wise system architecture for a basic medical instrumentation system is sketched out in this section . It is used to outline the common structures involved in such a system. This generic model is later further developed to map to the pacemaker system.

In the broadest sense, a medical instrumentation system would be comprised of the following four basic components, as illustrated in Figure 2.2:

- ***Measurand***: The physical quantity or condition that the instrumentation system measures is called the *measurand* (or *monitored variable*). The source for the measurand/monitored variable is the underlying physiological system.
- ***Sensor/actuator***: The sensor converts the intrinsic biosignal into an electrical signal that is recognized by the control system as the *monitored variable*.

Upon the reception of input from the sensor, the control system then processes the embedded information and outputs instructions that activate the actuator. The actions taken by the actuator – in the form of native biosignals– to act upon the biological system are physiologically specific to the associated biosystem. These induced actions taken by the actuator are known as the *controlled variable*.

- ***Control System:*** The Control System is at the centre of the medical instrumentation system. It is the ‘brain’ behind the intended operations performed by the medical device. Employment of microprocessors and their accompanying software enables the programmability of the medical device, as well as the automatic reading and control of sensors and actuators. A *feedback loop* is typically used in the control system circuitry to achieve the above-mentioned objectives. It is also preferable that the design of the control system should always promote minimal user intervention, calibration and set up.
- ***Output System:*** The output system comes in many forms. It could be as simple as a display, where representation of the physiological quantity is made visible on a computer screen, or on a scale, or on the chart of a recorder or in numerical form, just to mention a few. Other non-visual forms of displays are also used, such as audible alarms. In addition, output signals from the computerized control system can be passed to a persistent storage to maintain the data for future reference. The output data could also be transmitted to other parts of an integrated system or to another location using standard interface connections.

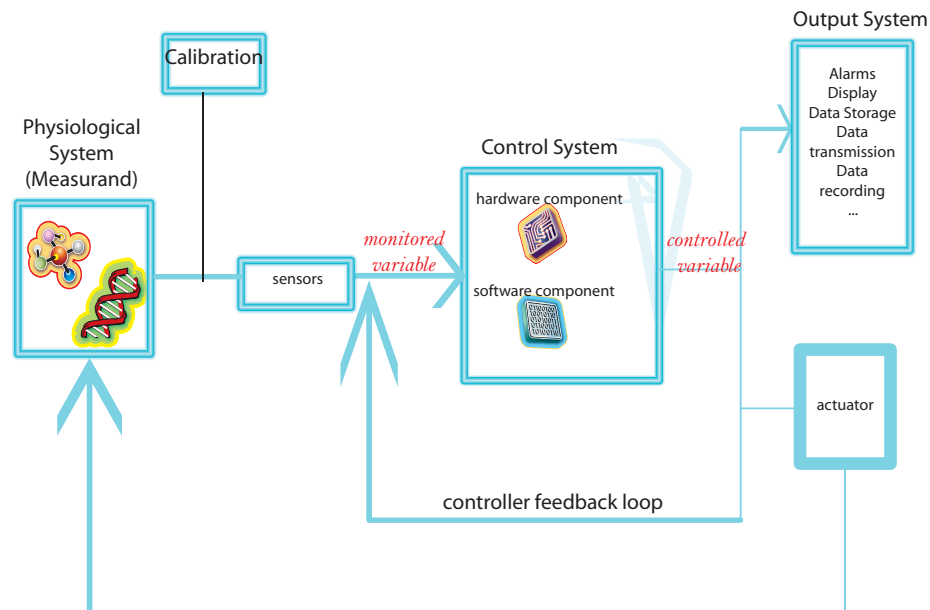


Figure 2.2: A basic medical instrumentation system as a control system.

Control system design at such levels of sophistication is an extremely involved process. Other issues embodied in a typical control design include:

- ***Modeling the physiological process:*** The biological properties of the physiological system are an intrinsic part of the control problem. Thus a control engineer needs to be familiar with the biology of the process under study. This includes a rudimentary knowledge of the basic anatomy and physiology of the system under study. The physical dimensions of various anatomic structures and how they relate to performance specifications must also be understood. Therefore, establishing an accurate model for the underlying biological system is a first step in designing medical control systems.
- ***Control objectives:*** It is important for system engineers to understand the

goal of their design, that is, to formulate the control objectives. This includes answers to the following questions:

- What does one want to achieve?
 - What variables need to be controlled to achieve these objectives?
 - What level of performance is necessary (accuracy, speed, ... etc.)?
-
- ***Calibration:*** In most medical instrumentation systems, some form of *calibration* is necessary at regular intervals. The calibration signal is usually applied to the sensor input or as early in the signal conditioning chain as possible [16].
 - ***Level and type of monitored variables:*** Measurements on the human body can be made at several levels of the functional systems and sub-systems. At the top level are measurements made on the human body holistically due to an accessible environment. Recording of ECG and measurement of body temperature are examples of such measurements. The next level of measurements is system-based. Measurements are made on the major functional systems of the body such as the cardiovascular and pulmonary systems. The functional system can be further sub-divided into sub-systems and organs and still smaller units down to the cellular and molecular levels [16]. Medical devices with different applications have monitored variables at all of these levels; each equipped with specially designed features and an appropriate degree of sophistication.
 - ***Communications:*** Connecting sensors to actuators involves the use of communication systems. The design of communication systems and their associated

protocols is an increasingly important aspect of modern control engineering. There are special issues and requirements for communication systems with real time data. The one that arises most frequently is the problem of delays. Although in some applications small delays can be safely ignored, in high speed real time control systems, these delays could be of major importance. In some technologies, such signal transmission delays are overcome by requiring the transmitter to resend the data at some later random time. This introduces a non-deterministic delay into the transmission of the data [12]. Since all control systems depend upon precise knowledge of, not only what has happened, but also when it happened, attention to such delays is very important for the performance of the overall system.

- **Algorithms:** Here, the term ‘*algorithm*’ specifically, and exclusively, refers to one particular piece of ‘*business/medical logic*’ that is encompassed by a medical device with a *separate* control algorithm. In other words, it is an algorithm that the device implements in order to perform some medical-related function, which is other than the control algorithm of the overall system. For example, in a pacemaker system, there are self-contained algorithms for searching for atrial flutter signals, algorithms for rate-adaptive pacing, and algorithms for automatic termination of tachycardia – each dealing with one distinct problem. All of these function-specific algorithms, together with the overall control algorithm of the system, determine the behaviour of the medical device as a whole – that is, they decide on the *relation* between the *monitored variables* and the *controlled variables* of the system.

- ***Disturbances and uncertainty***: As for all other real life systems, medical instrumentation systems are acted upon by noise and external disturbances. These impurities in the raw biosignal can have a significant impact on the performance of the system. However, by appropriate design of the control system, insensitivity to external disturbances can be achieved. In cases where the influence of a noise signal is inevitable, its extent and potential impact on the overall system behaviour must be properly documented.

Another related issue is that of model uncertainty. All real world systems are very complex, but an important property of feedback control is that one can often achieve the desired level of performance by using relatively simple models [12]. However, regardless of what model the medical system designer chooses to use in order to represent the underlying physiological system, uncertainties about the real biological environment will always exist in the design space. This is the gap between the real-world function and precise behaviour of the physiological system and its approximated model, bridged by implicit *assumptions* made about the environment.

2.6 General Constraints in Design of Medical Instrumentation Systems

Medical instrumentation systems are primarily used for *monitoring* and/or *controlling* physiological parameters of the human body. In situations where external interventions are required for diagnostic and treatment purposes, a stimulus or energy of

some kind is provided by the medical device as its calculated output, which is also known as the *controlled variable* of the system.

If we were to model a medical instrumentation system as a specialized control system that takes input from, and outputs signals to, its controlled environment – a physiological system within the human body in this case, then the design of such a medical system would be confined by the biological laws of nature of the underlying physiological system.

More specifically, general constraints in the design of such medical systems include [16]:

- ***Inaccessibility of the Signal Source***: One of the major problems in acquiring input signals from a living system is the difficulty in obtaining access to the source of the physiological variable being sensed. For example, installing a sensor in the human brain could be a daunting task. In addition, the physical size of many sensors may put an extra constraint on their use in the area of interest. In case of such inaccessible physiological variables, the input must be taken indirectly.
- ***Variability of Physiological Parameters***: Physiological variables sensed from the human body are rarely deterministic, as they are generally *time-variant* in a non-periodic fashion. In other words, input parameters vary widely among normal patients even when conditions are similar. Also, many internal anatomical variations exist among patients, resulting in variability of sensed biosignals from one patient to another. Therefore, the physiological variable must be represented by some kind of empirical, statistical and/or probabilistic

distribution function.

- ***Interference among Physiological Systems:*** Many feedback loops exist among physiological systems and many of the interrelationships amongst them contribute to this inherent variability of physiological signals. Simply put, stimulation of one part of a given system will normally affect all other parts of that system, sometimes even parts from a different, but connected, system. Moreover, unlike many complex non-medical systems, a biological system cannot be 'turned off' nor have parts of it removed during sensing to avoid interference from undesirable physiological signals.
- ***Sensor Interface Problems:*** All measurement/monitor systems are affected in some way by the presence of the measuring sensor. The problem is elevated even more when the sensor is used on a living system. Extra care needs to be taken while designing such interfaces to ensure that the loading effect of the sensor on the source of the monitored variable is minimal. In a word, the sensor should be minimally invasive and interface with the living system with minimum extraction of energy.
- ***High Possibility of Artifacts:*** The term artifact refers to an undesirable signal that is extraneous to the monitored physiological variable. *Cross talk* and *noise* generated within the sensing instrument are examples of possible artifacts. A major source of artifacts in medical instruments is due to the movement of the subject. Many sensors are sensitive to movement; therefore, movement of the subject gives rise to spurious signals, which may even be

significant enough to obscure the signal of interest.

- ***Safe Levels of Applied Energy***: The application of an external stimulus to living tissue imposes serious safety concerns. If not used well, the healing power of the medical instrumentation system could, instead, turn disastrous. Moreover, safe levels of various types of energy on the human subject are difficult to establish. Therefore, designers of medical systems must consult a vast number of clinical studies carried out by numerous researchers to help them establish the threshold of adverse affects by the applied energy, as well as identify the safe application range and tolerance for each output signal.
- ***Patient Safety Considerations***: Medical instruments are physically connected to the patient. Because of the prevalent use of electrical signals as the cardinal information carriers in medical systems, the possibility of an electric shock hazard is very strong unless adequate measures have been taken in the design of the equipment. Additionally, other non-technical personnel involved in the application of a medical instrument, such as medical or paramedical staff, may also be exposed to such safety hazards. Their safety needs to be ensured as well. In response to this resounding safety issue, various organizations at national and international level have prescribed specific guidelines and standards to entrench the safe and effective application of medical devices with human as subjects.
- ***Reliability Aspects***: Life saving equipment, such as defibrillators, is *safety-critical*; their failure or malfunction may result in a life-threatening or serious

injury to the patient. Performance requirements for such safety-critical systems dictate that the equipment must be reliable, simple to operate and capable of withstanding physical abuse due to transportation within the hospital or in the ambulances.

From a software point of view, software engineering for life-critical systems is particularly difficult. Several approaches are commonly used. The standard approach is to carefully code, inspect, document, test, verify and analyze the system. An alternative is to certify a production system, a compiler, and then generate the system's code from specifications. Another approach uses formal methods to generate proofs that the code meets requirements. All of these approaches improve the software quality in safety-critical systems by testing or eliminating manual steps in the development process.

- ***Human Factor Considerations:*** Human factor considerations arise as a result of the ever-increasing complexity of the medical devices/systems and their accompanying human-machine interfaces. Modern medical equipment usually requires a vast amount of information exchange between devices and the user in order to monitor and control the technical functions of the system. In contrast to this rising demand for machine-handling proficiency, medical staff often lack technical experience in working with complex electronic systems. Consequently, the desired or intended performance of the whole system may not be achieved. Hence, user interface design issues are finding themselves of increasing importance in the medical domain.

- ***Government Regulations:*** Because of the fact that medical devices impact human lives in the most profound way, their associated industry is one of the most regulated. National and international standards that prescribe rules and requirements on the safety, performance, design, operations, etc. of medical devices are promulgated as regulations by governments. These regulations and standards are introduced to ensure that the medical equipment performs its intended function and is safe to operate. Designers of medical instruments should therefore be fully conversant with all applicable regulations on a particular product or system. A detailed discussion on regulations concerning medical devices and their related issuing agencies is provided in the next section.

In summary, many factors impose constraints on the design of general medical instrumentation systems. Apart from these major influential factors, there are also several minor considerations, which need to be taken into account in the initial design and development stages. These include [16]:

Signal Consideration: Type of sensor, sensitivity, range, input impedance, frequency response, accuracy, linearity, reliability, differential or absolute input.

Environmental Considerations: Signal-to-noise ratio, stability with respect to temperature, pressure, humidity, acceleration, shock, vibration, radiation, etc.

Medical Considerations: Invasive or non-invasive technique, patient discomfort, radiation and heat dissipation, electrical safety, material toxicity, etc.

Economic Considerations: Initial cost, cost and availability of consumables and compatibility with existing equipment.

Needless to say, development for a commercial medical instrument is an extremely involved process. For starters, both generic and product-specific constraints, such as those listed above, that are associated with the particular type of medical device must be taken into consideration before the project is even launched for design and development. On top of that, in order to prevent system engineers from losing sight of further constraints posed by the underlying biological environment, a close association between the engineering design team and motivated medical professionals remains a key element to the success of the project. This collaborative association is invaluable not only during the development process, but also for the clinical trials of the product so developed.

2.7 Regulation of Medical Devices

The medical instrumentation industry in general and hospitals in particular are amongst the most regulated industries [16]. This is because of the special nature of the environment medical devices operate within. With human beings as the subject, precise functioning of a medical device is extremely critical. The existence of any uncertainty or non-determinism in the behaviour of such safety-critical systems could raise substantial concern regarding the overall safety of the device and the potential adverse effects posed on its patients.

When people's lives are at stake, it is difficult for the society or government not to impose some form of legal or contractual obligation to enforce patient safety. The result is the production of a vast pool of codes, standards and regulations,

either national or international, issued by various countries for different types of medical equipment and facilities. For example, spotlighted in this thesis is the “*FDA Regulatory Requirements for Medical Devices with Control Algorithms*” [7]. Among other things, the FDA regulatory requirements document addresses issues such as when a device is subject to FDA regulation, what steps should a device developer follow to comply with FDA regulations, and what process the device developer needs to follow when conducting tests and clinical trials.

Regulatory requirement for medical devices begins at or before the design phase for the device. Therefore, it is incumbent on system design engineers to acquire a firm grasp on the terms delineated in the corresponding documents and incorporate these requirements as early as possible during the design phase.

Before digging deeper into the details, a classification is given here to better distinguish among different types of regulatory documents. In [16], Singh defines the following terms:

Regulations: A regulation is an organization’s way of specifying that some particular standard must be adhered to. These are rules normally promulgated by the government.

Standards: A standard is a multi-party agreement for establishment of an arbitrary criterion for reference. Alternatively, a standard is a prescribed set of rules, conditions or requirements concerned with the definition of terms, classification of components, delineation of procedures, specifications of materials, performance, design or operations, measurement of quantity and quality in describing materials, products, systems, services or practice. Standards exist

that address systems (protection of the electrical power distribution system from faults), individuals (measures to reduce potential electric shock hazard) and protection of the environment (disposal of medical waste).

Codes: A system of principles or regulations or a systematized body of law or an accumulation of systems of regulations and standards. In general, a code is a compilation of standards relating to a particular area of concern. For example, state/provincial government health codes contain standards relating to providing health care to the state/provincial population.

Specifications: Documents used to control the procurement of equipment by laying down the performance and other associated criteria. These documents usually cover design criteria, system performance, materials and technical data.

Standards, codes and regulations may or may not have legal implications depending upon whether the promulgating organization is government or private.

2.7.1 Standards

Standards for medical devices can be further broken down into the following three types [16]:

Voluntary Standards: Developed through a consensus process where manufacturers, users, consumers and government agencies participate. They carry no inherent power of enforcement but provide a reference point of mutual understanding.

Mandatory Standards: Required to be followed under law. They are incumbent on those to whom the standard is addressed and enforceable by the authority having jurisdiction.

Proprietary Standards: Developed either by a manufacturer for its own internal use or by a trade association for use by its members. They can be adopted as voluntary or mandatory standards with the consensus/approval of the concerned agencies.

2.7.2 Regulatory Requirements

Since 1976, empowered by the Medical Device Amendments to the Federal Food, Drug and Cosmetic Act (FFDCA), the Food and Drug Administration (FDA) has been the principal ruling body to regulate nearly every facet of the manufacture and sale of medical and diagnostic devices. The FDA is a consumer protection agency. For medical devices, the role of the FDA is to “protect against hidden defects from design and composition, manufacturing and handling, and biological effects” [7].

“Medical Device” is defined in the FFDCA, [9], as “any item promoted for a medical purpose that does not rely on chemical action to achieve its intended effect”. These devices are further categorized into three classes in [9] based on the principle that devices that pose greater potential hazards should be subject to more regulatory requirements.

Class-I

General Controls: A device for which the controls authorized by law are sufficient to provide reasonable assurance of the safety and effectiveness of the device. Manufacturers are required to perform registration, pre-marketing notification, record keeping, labeling, reporting of adverse experiences and good manufacturing practices. These controls apply to all three classes.

Class-II

Performance Standards: Apply to devices for which general controls alone do not provide reasonable assurance of safety and efficacy, and for which existing information is sufficient to establish a performance standard that provides this assurance. However, until performance standards are developed by regulation, only general controls apply.

Class-III

Premarket Approval: Applies to devices which are used to support or sustain human life or to prevent impairment of human health, devices implanted in the body and devices which present a potential unreasonable risk of illness or injury. These are highly regulated devices and require manufacturers to prove their safety and effectiveness prior to their market release.

According to the above classification and definitions, a pacemaker system would

be classified as a Class-III medical device. Class-III devices are also *'high-risk'* devices. The Quality System Regulation (QSR) [7], requires medical device manufacturers to use a design validation process for high-risk devices. The design validation process examines the design inputs and assures that the design outputs meet the requirements of the patient and the user. For devices with control algorithms, it is also required that an applicant to the FDA must provide details of the control algorithm, how it was implemented, and the results of studies supporting the intended use of the device.

2.7.3 Standards Related Agencies

In most countries, domestic agencies exist to set and enforce standards, however, driven by the great power of globalization, there has been a pressing urge in the international community for adoption of uniform standards which could be applicable across national boundaries. In light of this pending demand, two organizations at the international level are active in the area of standardization.

International Electro-technical Commission (IEC): Deals with all matters relating to standards for electrical and electronic items. One of the notable standards developed under IEC is 60601-1, *Safety of Medical Electrical Equipment, Part-I: General Requirements for Safety* (1988), [21], and its Amendment (1991) and the document 60601-1-1, *Safety Requirements for Medical Electrical Systems* [22].

International Organization for Standardization (ISO): ISO oversees aspects

of device standards other than those related to electro-technology. The purpose of the ISO is to facilitate the international exchange of goods and services and to develop mutual cooperation in intellectual, scientific, technological and economic ability.

It is noteworthy that the pool of agency-promulgated regulations and standards does not end here. Apart from the major players in the field, there are hundreds of other agencies that enact regulations and standards in the areas of electrical safety, technology management, occupational safety, radiology, bio-safety, clinical laboratories, etc. In addition, there are thousands of voluntary standards, clinical practice guidelines, and government laws – all applicable to medical devices. Therefore, biomedical engineers are advised to consult all the relevant international/national standards and regulations for the effective design and implementation of medical devices.

Chapter 3

Artificial Cardiac Pacemaker as a Medical System

When one takes the notion of a generic medical instrumentation system and project it onto an artificial cardiac pacemaker, the resultant realization is a device that inherits all of the general properties of its parent. That is to say, a cardiac pacemaker system is not only built on the same technological foundation shared by all medical devices, it is also constrained by the same set of rules (and assumptions), environmental or non-environmental, that are applicable across the genre. This chapter is an extension of the previous one, featuring a specific type of medical device that is the ‘heart/centre of attention’ of this thesis – the artificial cardiac pacemaker system.

Defined in terms of functionality, a pacemaker is “*an electronic medical device implanted in the human body that delivers electrical stimuli over leads with electrodes in contact with the heart.*” [25]. Examining this definition closely, one could

develop the following derivatives, namely:

1. The internal part of a pacemaker system consists of two parts: a component that generates electrical stimuli – the *pulse generator* – and *leads* with attached electrodes that deliver the stimuli.
2. The type of monitored variable for the pacemaker control system, is *in vivo* – its acquisition takes place inside a living organism, at an organic level.
3. The type of biomedical signal used in the pacemaker system is a *bioelectric* signal.
4. The biological organ involved in the operation of a pacemaker device is the *human heart*.
5. The physiological system a pacemaker device interacts with is the *Cardiovascular system*.

Enlightened by the above findings, this chapter directs its focus towards the exploration of the biological habitat of a pacemaker device, with the mission of identifying potential environmental assumptions.

3.1 Anatomy of the Heart

The basic interior anatomy of the human heart is illustrated in Figure 3.3. The two anatomical structures that are important to the pacemaker device are the *Right Atrium (RA)* and *Right Ventricle (RV)*, as these are the two chambers where the

electrodes (electrical contacts) are implanted, as shown by the arrangement in Figure 3.4.

Two other prominent structures that deserve immediate attention are the two electric-pulse-generating, conduction nodes: the *Sinoatrial (SA) node*, located at the top of the right atrium, and the *Atrioventricular (AV) node*, located between the right atrium and right ventricle. These two nodes are part of the intrinsic electrical conduction system of the heart, and are known as the ‘*natural*’ cardiac pacemakers.

In order not to confuse the term ‘natural pacemaker’ with the artificial pacemaker device that is at the center of interest in this thesis, all references to the word ‘pacemaker’ in this thesis specifically refer to an artificial pacemaker device, unless otherwise stated.

3.2 The Electrophysiology of the heart

Two types of cells are found in the heart – *electrical cells* and *myocardial (mechanical) cells*. Electrical cells form the *electrical conduction system* of the heart, whereas the myocardial cells form the bulk musculature of the heart. Because of their special ability to initiate and transmit electrical signals, electrical cells are the fundamental building blocks of the heart’s natural pacemaker tissues, such as the SA node and the AV node.

The electrical conduction system helms the generation and delivery of instructions throughout the heart, while muscles or tissues react to these biosignals in form

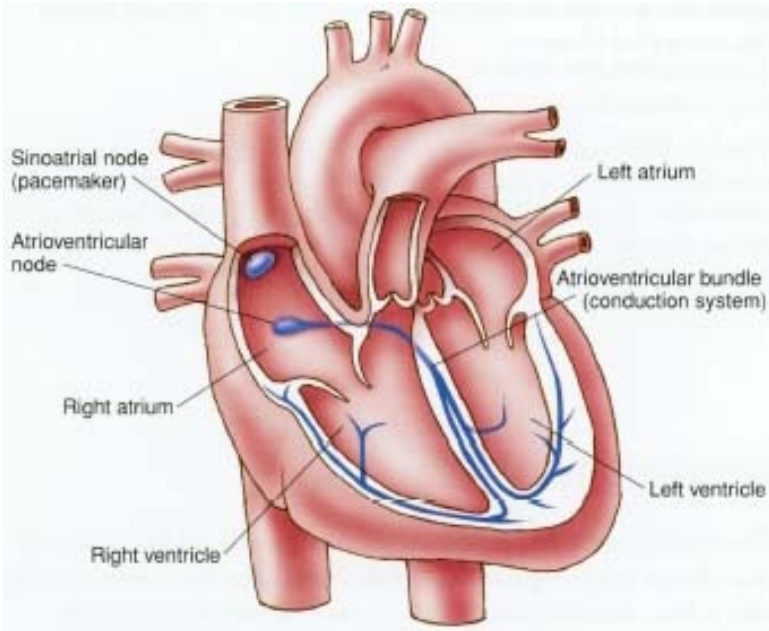


Figure 3.3: Interior anatomy of the human heart [5].

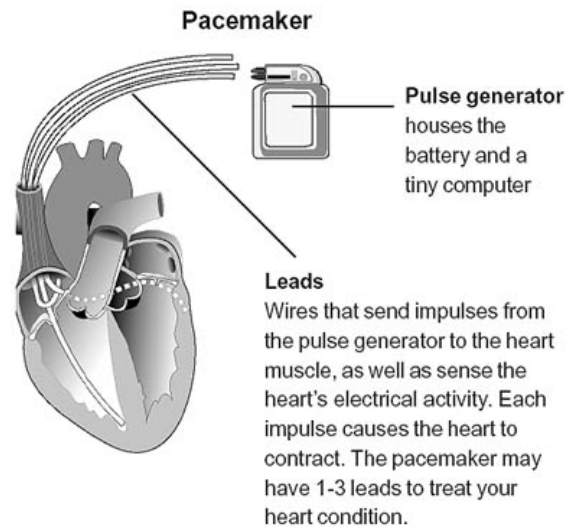


Figure 3.4: Structure of the implantable part of a pacemaker system, and its arrangement inside a patient's body.

of rhythmic contractions. It is this highly coordinated interaction between the electrical stimuli and the mechanical action of the myocardial muscles that enables the effective pumping of the heart. Damage in either one of the two systems can cause the malfunction of the other. If the electrical system of the heart fails to function properly, for example, due to blockage of the conduction pathway, *arrhythmias*, which are mechanical activities, may occur as a manifestation.

3.2.1 The Electrical Conduction System of the Heart

The main function of an artificial pacemaker is to regulate the heartbeat of patients exhibiting *Bradycardia* (a very slow heart rhythm), by interfering with the electrical conduction system of the human heart. The natural electrical conduction system

of the heart orchestrates the contractions of the myocardium (cardiac muscle) with electric impulses generated by the Sinoatrial (SA) Node. Electrical activity in the heart is best described in terms of the *Conduction Pathway*.

The Conduction Pathway

Figure 3.5 illustrates the important features of the electrical conduction system of the heart. Electrical signals initiated at the SA node are propagated throughout the myocardium passing various conduction nodes through a conduction pathway. This conduction pathway can be summarized as follows:

Sinoatrial node (SA node) \rightarrow <via *internodal pathways*> \rightarrow
Atrioventricular node (AV node) \rightarrow <via *Bundle of His*>
 \rightarrow **Purkinje fibers**/ventricular myocardium

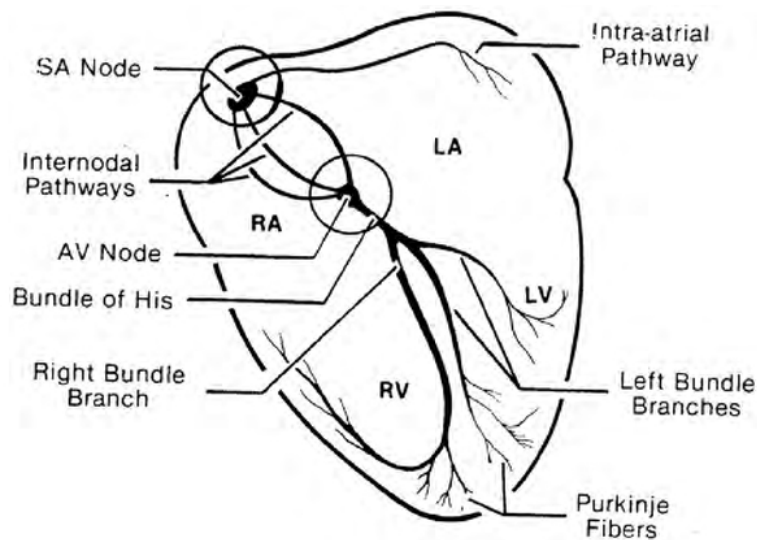


Figure 3.5: The Electrical Conduction System of the heart. (Image adapted from [8])

Signals arising in the SA node stimulate the atria to contract before traveling to the AV node. As electrical activity is spreading throughout the atria, it travels via specialized tracts, known as *internodal pathways* (literally, between nodes), from the SA node to the AV node. After a delay, the stimulus is conducted through the *bundle of His* to the *Purkinje fibers* and the *endocardium* at the apex of the heart, then finally to the ventricular epicardium [6].

The delay at the AV node is crucial, as it allows enough time for all of the blood in the atria to fill their respective ventricles. This AV-interval is one of the many programmable timing intervals found in modern day pacemakers. It is also one of the four fundamental timing intervals that constitute the grounds on which an artificial pacemaker's functionality is built.

3.2.2 The Pacemaker Site

Even though the SA node is most frequently recognized as the origin of the electrical signal present along the conduction pathway, almost all of the components in the cardiac conduction system – i.e., SA node, AV node, Bundle of His, left and right branches of this bundle, and Purkinje fibres – are able to initiate a spontaneous action potential, provided that they are not inhibited by other electrical activity.

The SA node is the most important cardiac pacemaker; it contracts with the fastest rate and is responsible for the whole heart's beat. Because of its special importance, the SA node is known as the *primary pacemaker*. The cardiac electrical conduction system is so designed such that, in case one pacemaker fails, there would always be some other pacemaker further down the conduction pathway to pick up the

responsibility of producing an electric signal. The AV node, known as the *secondary pacemaker*, pulsing at a slower rate, acts as a backup to the primary pacemaker.

Even further down the electrical conduction pathway, the Bundle of His, the left and right branches of this bundle, and the Purkinje fibres form the group of *tertiary pacemakers*.

Table 3.2 summarizes the characteristics of the heart's natural pacemakers in all three categories.

Table 3.2: Natural Cardiac Pacemakers and their Characteristics

<i>Type</i>	<i>Tissue(s)</i>	<i>Firing Rate (per minute)</i>	<i>Primary characteristics</i>
<i>Primary pacemaker</i>	SA node	60-100	The SA node is the heart's pacemaker.
<i>Secondary pacemaker</i>	AV node	40-60	An impulse from the AV junction can take over if the SA node should fail.
<i>Tertiary pacemaker</i>	Bundle of His, the left and right branches of this bundle, and Purkinje fibres	20-40	If the AV junction also fails, the ventricular (tertiary) pacemakers can take over.

3.2.3 Requirements for Effective Pumping

Owing to the exquisite intricacy of the heart's electrophysiology, a set of requirements exists on the cardiac electrical conduction system for the effective functioning of the

heart.

The objective is to maximize efficiency of myocardium contraction and cardiac output. In order to achieve this objective, the cardiac electrical conduction system is required to have:

- **A substantial atrial to ventricular delay.** This *AV delay* plays a crucial part in achieving the synchrony between the atria and the ventricles. It allows the atria to fully empty their contents into the ventricles and prevents inefficient filling and back flow. The AV delay is accomplished by having the atria electrically isolated from the ventricles, connected only via the AV node, which acts as a delay in the conduction path, introducing the desired time interval.
- **Coordinated contraction of ventricular cells**, which in turn requires that:
 - Ventricular contraction begins at the apex of the heart, progressing upwards to eject blood into the great arteries.
 - Depolarization propagates through cardiac muscle very rapidly. In other words, cells of the ventricles contract nearly simultaneously.
 - The action potentials of cardiac muscle are sustained. This prevents premature relaxation, maintaining initial contraction until the entire myocardium has had time to depolarize and contract.

- **Absence of tetany**¹. A *refractory period* must be enabled for the myocardium to relax after a contraction. Any further stimulus to the heart muscle during this refractory period should not result in a sustained contraction. Sustained contraction of the heart without relaxation would be fatal, and this is prevented by a temporary *inactivation* of certain ion channels.

3.3 The Cardiac Cycle

The heartbeats a pacemaker is made to regulate are formally referred to as *cardiac cycles*. Cardiac cycle is the term referring to “all or any of the events related to the flow of blood that occur from the beginning of one heartbeat to the beginning of the next.” [14] The frequency of the cardiac cycle is the heart rate.

A normal cardiac cycle consists of three major stages: *atrial systole*, *ventricular systole* and *complete cardiac diastole*. The term *diastole* is synonymous with relaxation of a muscle. Thus, one cardiac cycle is one contraction of the heart plus the relaxation period that follows.

Cardiac diastole is the period of time when the heart relaxes after contraction in preparation for refilling with circulating blood. *Ventricular diastole* is when the ventricles are relaxing, while *atrial diastole* is when the atria are relaxing. Together they are known as *complete cardiac diastole*.

¹Tetany: a condition marked by intermittent muscular spasms, caused by malfunction of the parathyroid glands and a consequent deficiency of calcium.

3.4 The ECG: Recording Heart Activity

“An **electrocardiogram** (*ECG*) is a test that measures the electrical activity of the heart. This includes the rate and regularity of beats as well as the size and position of the chambers, any damage to the heart, and effects of drugs or devices to regulate the heart (such as a pacemaker).” [19]

3.4.1 Heart Electrical Forces

During the cardiac cycle, electrical changes – manifested by variations in action potential, usually on a milli-volts scale – take place in the heart. Being able to record and visualize these electrical potential variations over time has great clinical significance.

Detection of electrical forces in the heart.

Electrical forces in the heart can be detected on the body’s surface. Therefore, electrodes attached to the patient’s skin can detect electrical forces in the heart.

Recording of electrical forces in the heart.

The *electrocardiograph* is the biomedical recorder used to record the electrical changes of the heart. An electrocardiogram, or ECG, is a graphic produced by an electrocardiograph, which records the electrical activity of the heart over time.

In summary, electrical signals in the heart characteristically precede the normal mechanical action of the myocardium, providing effective control of the heart’s function. Also, monitoring of these signals has great clinical significance, especially in

determining the effectiveness of a heart-regulatory device such as a pacemaker.

3.4.2 ECG Waves and Intervals

A normal heartbeat (or cardiac cycle) manifests itself on an ECG as a series of up and down waves, as shown in Figure 3.6, called *deflection waves*, corresponding to the three stages in a cardiac cycle. These connected wave patterns, together, represent one complete cardiac cycle beginning with the heart's natural pacemaker impulses and including ventricular repolarization.

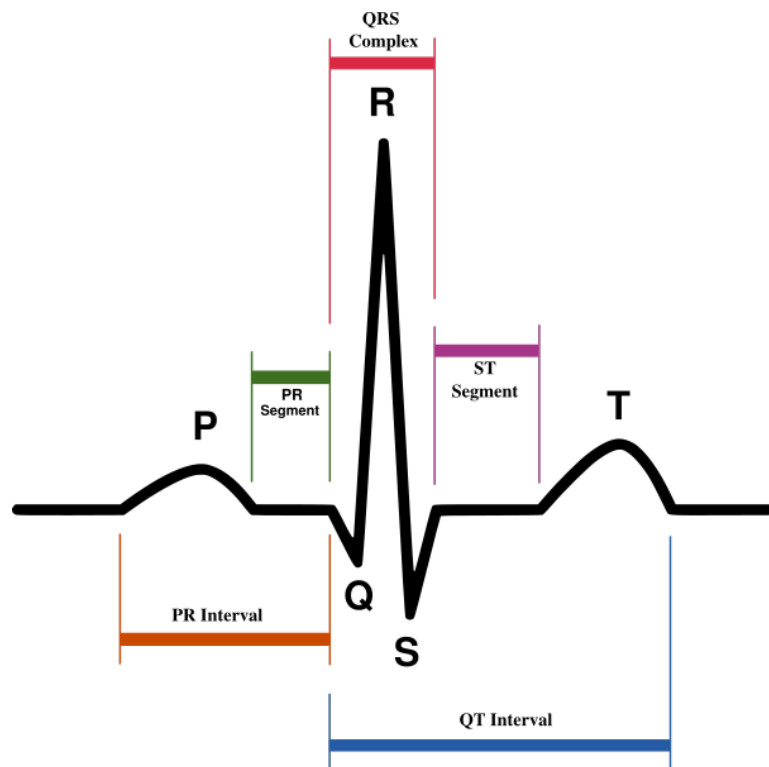


Figure 3.6: Schematic representation of normal ECG [1]

The size of the deflection waves, and especially the time intervals between them, has special significance in interpreting cardiac rhythm and diagnosing rhythm disorders in the cardiac conduction system. More importantly, they are important tools in specifying the behaviour of a pacemaker system, or for that matter any medical device related to the heart.

Pacemaker design engineers and medical staff use these ECG waves and time intervals so extensively that they form an essential part of their common vocabulary during communication. It is usually the case that a thorough understanding of the waves and intervals involved in a cardiac cycle is a prerequisite (and usually an underlying presumption made by system design engineers) for the successful communication between various roles in the development of a pacemaker system.

Without further ado, the important ECG waves and time intervals, along with their associated electrical activity and graphic depiction, are summarized in Figure 3.7.

In short, a typical ECG tracing of a normal heartbeat consists of a P wave, a QRS complex, and a T wave.

SA Node: P Wave

The *P wave* is the small upward (positive) wave on an ECG that indicates atrial polarization (the spread of an impulse from the SA node through the muscle of the two atria). During normal atrial depolarization, the main electrical vector is directed from the SA node towards the AV node.

- **Normal duration:** between 0.06 and 0.1 seconds.


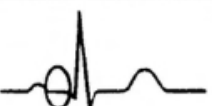
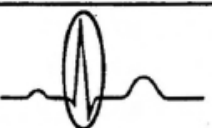
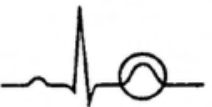
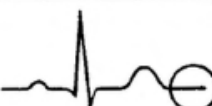
Electrical Activity	Graphic Depiction	Associated Pattern
Atrial Depolarization		P Wave
Delay at AV Node		PR Segment
Ventricular Depolarization		QRS Complex
Ventricular Repolarization		T Wave
No electrical activity		Isoelectric Line

Figure 3.7: Electrocardiogram wave patterns produced by electrical activity in the heart. (Image adapted from [8])

- **Normal height:** no more than 3 mm.

AV Node/Bundles: PR Interval

Measured from the beginning of the P wave to the beginning of the R wave, the *PR segment* represents much of the delay in the AV node and part of atrial repolarization/refractorization.

- **Normal duration:** between 0.12 and 0.20 seconds.

Purkinje Fibers/Ventricular Myocardium: QRS Complex

The spread of electrical activity through the ventricular myocardium produces the *QRS complex* on the ECG.

- **Normal duration:** less than 0.12 seconds.

Ventricular Repolarization: T Wave

The *T wave* represents the last event of the cardiac cycle – the repolarization of the ventricles.

The Refractory Period

During this period, cell charges are depolarized and have not returned to their polarized state. A cell that is electrically ‘*refractory*’ cannot receive another impulse until it is repolarized. The refractory period on an ECG includes the QRS complex and the T wave. The *absolute refractory period* includes the QRS and the upslope of the T wave and is **NOT** a dangerous period. The *relative refractory period*, which

is the last half of the T wave, may allow depolarization of ventricles. It is dangerous if an impulse occurs at this time.

3.5 Pacemaker Indications and Contraindications

The indications and contraindications for permanent pacemaker implantation are specified in the clinical guideline published by the American College of Cardiology (ACC) and the American Heart Association (AHA). After its first publication in 1984, three subsequent revisions of the original guideline have been released, the latest being the 2002 update in collaboration with the North American Society of Pacing and Electrophysiology (NASPE). In [13], Gabriel outlines the indications and recommendations for pacemaker therapy based on the latest guideline. The full set of Guidelines will not be reproduced here; for highlights of features, please refer to [10, 13].

What is worth mentioning here, however, is the interrelation between innovation in pacemaker technology and the corresponding set of indications and contraindications it permits. Interestingly, the relation between technological advances in pacemakers and its indications is not strictly positive. In some cases, newer technology promotes the treatment of new diseases and conditions; in others, conversely, existing indications have atrophied as a result of technological progress. An example of the former situation is the advent of rate-adaptive pacing, which has allowed a cure for patients with chronotropic incompetence.

Chapter 4

Operational Characteristics of an Artificial Pacemaker

This chapter addresses the following issues/concepts:

- The Programmability of the pacemaker; the basic set of programmable variables and their effects
- Functional behaviour of a (simple) DDD pacemaker, described in terms of nine DDD Timing Cycles
- Crosstalk and crosstalk intervals
- Upper Rate Response of DDD pacemakers

Modern day pacemakers are small, reliable and long-lasting units with a lot of possibilities regarding the mode of stimulation.

The pacing lead functions as a “two-way street” for the transmission of electricity to the heart for pacing as well as for the sensing of spontaneous cardiac electric activity from the heart to the pacemaker. The operative techniques and intraoperative measurements are straightforward compared to the technical knowledge required to understand the electrophysiology of pacing and to practice the best use of the important programmable functions when following up with patients. The function of an implanted pacemaker can be altered by means of a programmer, which is a type of dedicated desktop computer. A modern pacemaker lasts 7-10 years. When the battery is depleted, the entire pacemaker (excluding the leads) is replaced.

4.1 Terminology and Basic Concepts

Automatic Interval and Escape Interval

Escape Interval: The interval between an escape beat and the normal beat preceding it.

In practice, the escape interval is measured from the onset of the sensed QRS complex in the surface ECG. The escape interval measured in this way must necessarily be longer than the electronic escape interval because intracardiac sensing takes place a finite time after the onset of the surface ECG.

Automatic Interval: The interval between two consecutive pacemaker stimuli.

In other words, the Automatic Interval is the stimulus-to-stimulus interval.

Note that

- WITHOUT HYSTERESIS the automatic interval equals the escape interval.
- WITH HYSTERESIS the escape interval is longer than the automatic interval.

Timer, Output Circuit, and Sensing Circuit

Timer : determines the interval between stimuli.

Output Circuit : determines amplitude and duration of stimuli.

Sensing Circuit : consisting of an amplifier, a filter, and a level detector, the sensing circuit takes the heart signal as input and outputs a signal to the timer for pacing the heart.

4.2 Types of Implantable Pacemakers

Depending upon different clinical applications, various *pacing modalities* are available in pacemakers. These pacing modes are classified according to:

1. the chamber(s) paced
2. the chamber(s) sensed
3. the pulse generator's response to sensing
4. the type of rate modulation

Further advancements in pacemaker technology have extended this list to include a fifth factor indicating the pacemaker's *anti-tachycardia functions*.

Classification Codes for Pacemakers

A five-letter-code nomenclature has been developed, and was jointly adopted by the North American Society of Pacing and Electro-physiology (NASPE) and the British Pacing and Electro-physiology Group (BPEG), as a standard to classify the type and functions of a pacemaker [2]. Table 4.3 displays this five-letter pacemaker identification system ¹.

Table 4.3: The NASPE/BPEG Generic (NBG) Pacemaker Code

I Chamber(s) Paced	II Chamber(s) Sensed	III Response to Sensing	IV Programm- ability, Rate Modulation	V Anti-tachy- arrhythmia Function(s)
O = None A = Atrium	O = None A = Atrium	O = None T = Triggered	O = None P = Simple Pro- grammable	O = None P = Pacing
V = Ven- tricular	V = Ventric- ular	I = Inhibited	M = Multipro- grammable	S = Shock
D = Dual (A+V)	D = Dual	D = Dual	C = Communi- cating	D = Dual (P+S)
S = Single (A or V)	S = Single		R = Rate modu- lation	

¹Note: Positions I-III are used exclusively for anti-bradyarrhythmia function; The PACE-MAKER System is a previous generation pacemaker, such that it does not support the anti-tachycardia functions. As a result, it uses a 4-letter-code system instead.

Different Types of Pacemakers

The electro-physiological arrangements of different types of implantable pacemakers are summarized in Figure 4.8, along with their corresponding NASPE/BPEG codes. Important characteristics of a set of commonly used pacemakers are described in this section:

Fixed Rate Pacemaker (VOO): This type of pacemaker is intended for patients with permanent heart blocks. It delivers stimuli to the heart at a pre-set rate. Changing of pacing rate is done externally by magnetically actuating a built-in relay. Because functioning at a fixed rate makes the pacemaker automatically ignore any intrinsic cardiac signal of the patient, it poses the danger of “*pacing with competitive rhythm*”, which is a term referring to the hazardous competition between the patient’s natural cardiac rhythm and that of the pacemaker.

Demand Pacemaker: Demand pacemakers are *non-competitive* – they eliminate the danger of pacing with competitive rhythm by specifying a **Lower Rate Limit (LRL)**, or **Lower Rate Interval (LRI)**. In a ventricular-based, lower rate timing system, the pacemaker only paces when the intrinsic R-R interval exceeds the specified LRL/LRI. The timer circuit in the pulse generator unit is responsible for keeping track of time; it determines the interval between stimuli.

QRS Complex Triggered Pacemaker (VVT): A QRS Triggered, or ventricular synchronized, demand pacemaker is designed to treat patients who suffer from general heart block but with occasional sinus rhythm. This type of

pacemaker both senses and paces in the right ventricle. A spontaneous QRS complex detected by the pacemaker will trigger an output during ventricular depolarization and reset the timer. In the case of asystole², a scheduled stimulus will be delivered to the ventricle after the specified LRI.

Ventricular Inhibited Pacemaker (VVI): A VVI pacemaker is meant for patients who generally have an intrinsic sinus rhythm but suffer from occasional heart block. As indicated by its mode code, in a VVI pacemaker, a spontaneous QRS complex detected by the pacemaker will automatically inhibit any scheduled output of the pulse generator and reset the timer. Therefore, in the VVI mode, a competitive rhythm is not possible. Moreover, the lifetime of the battery is extended because the pacemaker is not pacing during long periods of time in the presence of a spontaneous sinus rhythm.

Atrial Triggered Pacemaker: In atrial triggered pacemakers, detection of an atrial depolarization will cause the pacemaker to initiate an **Atrioventricular Interval (AVI)** – a time delay corresponds to the PR interval – only after which a stimulus is delivered to the ventricle. This kind of pacemaker is preferred when maximum augmentation of cardiac output at changing atrial rates is desired to meet various physiological requirements. Note that, compared to ventricular-triggered pacemakers, atrial-triggered pacemakers require higher *sensitivity*, i.e. a lower threshold in milli-volts, because P waves have lower amplitudes than R waves.

²*Asystole* is a state of no cardiac electrical activity, hence no contractions of the myocardium and no cardiac output or blood flow.

Dual Chamber Pacemakers (DDD, DDDR, DDI, etc.): Dual-chamber pacemakers are specifically indicated for treatment of conduction disorders that require restoration of rate and of atrioventricular synchrony, including varying degrees of AV block; low cardiac output or congestive heart failure related to bradycardia; and certain tachyarrhythmias [25]. In dual-chamber pacemakers, both atrium and ventricle are sensed and paced while maintaining a desired synchrony between the two chambers.

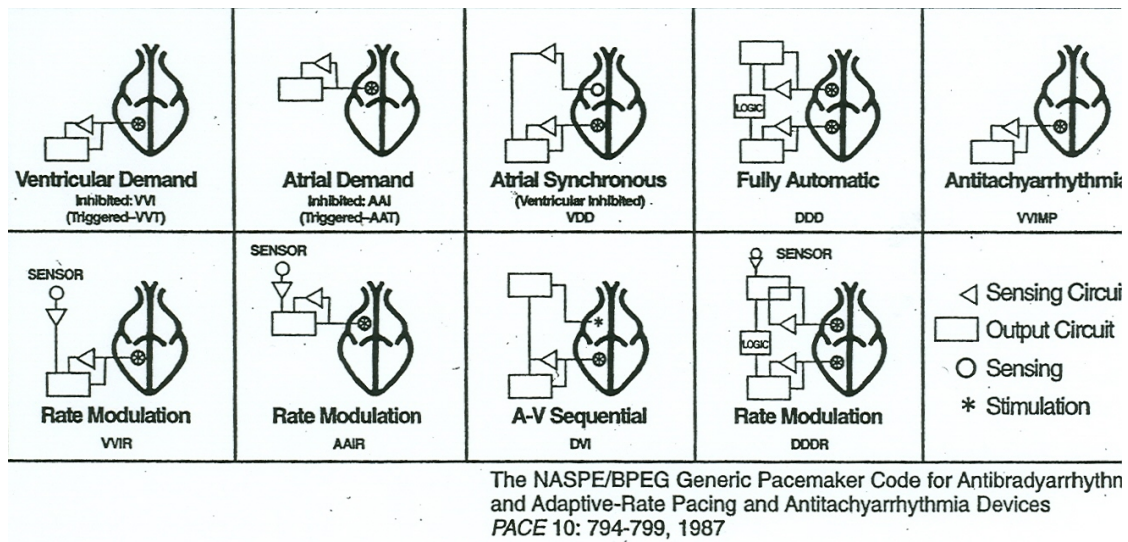


Figure 4.8: Various pacing modes in demand pacemakers and their corresponding NASPE/BPEG codes. [image adapted from [2]]

The required set of programmable pacing modes for the PACEMAKER System is specified in section 3.5 of [25].

4.3 Programmable Pacemaker

Modern pacemakers are extremely sophisticated and highly programmable. Microprocessors offer a high degree of flexibility and allow a wide range of products to be developed with new software and offer the possibility of faster revision of pacemaker function [16].

The basic programmable variables and their effects are described here.

Rate

Increase (a) To optimize cardiac output; (b) to overdrive or terminate tachyarrhythmias; (c) to adapt to pediatric needs; (d) to test AV conduction in AAI pacemakers; (e) to confirm atrial capture using the AAI mode by observing concomitant increase in the ventricular rate; (f) rate drop response for the treatment of vasovagal syncope. An abrupt fall in the spontaneous rate causes pacing at a higher rate (than the low basic pacing rate) for a given duration.

Decrease (a) To assess underlying rhythm and dependency status; (b) to adjust the rate below the angina threshold; (c) to allow the emergence of sinus rhythm and preservation of atrial transport; (d) to test sensing function; (e) sleep mode to provide a lower rate during the expected sleep time. Some devices use an activity sensor to drop the rate automatically with inactivity.

Output

Increase To adapt to pacing threshold

Decrease (a) To test pacing threshold; (b) to program pacemaker according to chronic threshold to enhance battery longevity; (c) to reduce extra cardiac stimulation (voltage rather than pulse duration) of pectoral muscles or diaphragm; (d) to assess underlying rhythm and dependency status.

Sensitivity

Increase To sense low amplitude P or QRS electrograms.

Decrease (a) To test sensing threshold; (b) to prevent T wave or after potential sensing by ventricular channel; (c) to avoid sensing extra cardiac signals such as myopotentials.

Refractory period

Increase (a) Atrial: to minimize sensing of the far-field QRS during AAI pacing. (b) Ventricular: to minimize T wave or after potential sensing by the ventricular channel

Decrease (a) to maximize QRS sensing; (b) to detect early ventricular premature beats

Hysteresis In the VVI mode to delay onset of ventricular pacing to preserve atrial transport function

Polarity

Conversion to unipolar mode (a) To amplify the signal for sensing when the bipolar electrogram is too small; (b) to compensate temporarily for a defect in the other electrode

Conversion to bipolar mode (a) To decrease electromagnetic or myopotential interference; (b) to evaluate oversensing; (c) to eliminate extracardiac anodal stimulation

AVI

Increase or Decrease to optimize LV function (a) Differential: to permit a longer interval after an atrial paced event than a sensed atrial event
(b) Rate-adaptive: to shorten the AV delay with an increase in heart rate

PVARP

Increase To prevent sensing of retrograde P waves

PVARP extension after a VPC

On/Off To prevent sensing of a retrograde P wave after a VPC

Postatrial ventricular blanking period

Increase To prevent crosstalk

Ventricular safety pacing

On/off To guarantee ventricular stimulation in the presence of crosstalk

Separately programmable upper rate

URI > TARP To provide a smoother upper rate response and avoid abrupt slowing of the ventricular rate when $\text{URI} = \text{TARP}$

4.4 The Output Pulse of the Pacemaker

Figure 4.9 depicts the waveform of a pacemaker output signal.

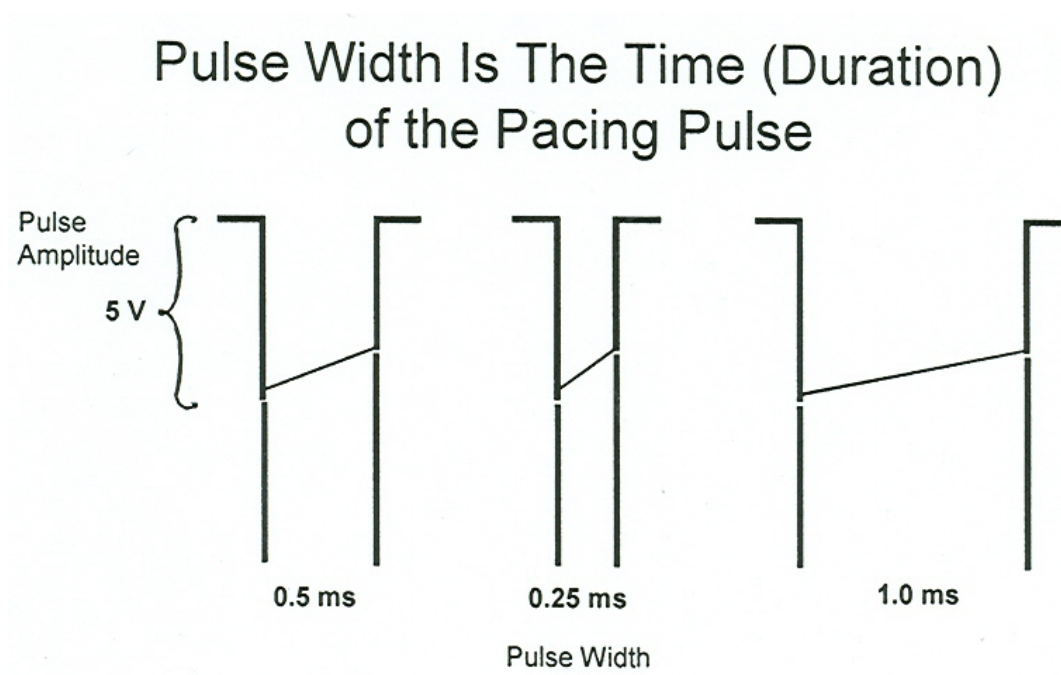


Figure 4.9: The output pulse of the pacemaker.

It is important to understand that the voltage of a permanent pacemaker refers to the amplitude of the *leading edge*, which is always constant. It is actually closer to 5.4 V (as opposed to the 5 V indicated in the diagram), because the lithium iodine cell generates a voltage of 2.8 V which is then doubled electronically. The *droop* is

influenced by a variety of factors, but visualization of the droop and the *trailing edge* is not required for the management of patients. The process does not terminate with the trailing edge. The pacemaker stimulus charges the electrode-tissue interface to a substantial voltage (polarization voltage) which is subsequently dissipated over a much longer period than the brief pacemaker stimulus. It is vital to acknowledge the existence of this “afterpotential” because it can play a role in problems associated with *oversensing*, i.e. unintended sensing of certain events.

4.5 Operational Characteristics of a simple DDD pacemaker

4.5.1 Ventricular Channel

As in a standard VVI pacemaker, the ventricular channel of an AV universal (DDD) pacemaker requires two basic timing cycles: the lower rate interval (corresponding to the programmed lower rate) and the ventricular refractory period. *The lower rate interval (LRI)* of a DDD pacemaker is the longest interval between consecutive ventricular stimuli without an intervening sensed P wave or from a sensed ventricular event to the succeeding ventricular stimulus without intervening sensed P wave. The *Ventricular refractory period (VRP)* is traditionally defined as the period during which the pacemaker is insensitive to incoming signals.

4.5.2 DDD pacing or VVI pacing with an atrial channel

Here the pacemaker acquires an atrioventricular interval (AVI) and an upper rate interval. The AVI is the electronic analog of the PR interval and is designed to maintain AV synchrony between the atria and the ventricles. The AV interval starts from the atrial stimulus and extends to the following ventricular stimulus or it starts from the point when the P wave is sensed and also terminates with the release of the ventricular stimulus. “Atrial tracking” is a term used to describe the response of a dual chamber pacemaker to a sensed atrial event which leads to the emission of a ventricular output pulse. The *Upper rate interval* is the speed limit to control the response of the ventricular channel to sensed atrial activity. For example, if the upper rate interval is 500 ms, a P wave occurring earlier than 500 ms from the previous atrial event will not be followed by a ventricular stimulus.

4.5.3 Derived timing cycles

The four basic timing cycles of a simple DDD pacemaker as already explained consist of: lower rate interval (LRI), ventricular refractory period (VRP), AV interval (AVI) and upper rate interval (URI). Additional timing intervals can be derived from these four basic intervals.

4.5.4 Atrial refractory period

It is axiomatic that the atrial channel of a DDD pacemaker must be refractory during the AV delay to prevent initiation of a new AV delay before completion of an AV

delay already in progress.

1. The postventricular atrial refractory period (*PVARP*) begins immediately after the emission of a ventricular stimulus and is the same after a ventricular stimulus or a sensed ventricular signal. An atrial signal falling within the *PVARP* cannot initiate a programmed AV interval.
2. The total atrial refractory period (*TARP*) is the sum of the AV delay and the *PVARP*. The duration of the *TARP* always defines the shortest upper rate interval or the fast paced ventricular rate.

4.5.5 *Upper rate interval* vs. *PVARP* as a basic interval

PVARP is considered as a basic interval controlling the upper rate. In this way the upper rate interval can be demoted to a derived interval. This manipulation converts the upper rate interval of the DDD pacemaker or the *TARP* ($AVI + PVARP$) to a derived function.

4.5.6 The six intervals of a simple DDD pacemaker

According to the above concepts, we now have a DDD pacemaker working with four basic intervals – LRI, VRP, AVI, and *PVARP*– and two derived intervals – Atrial Escape Interval, and the *TARP* = upper rate interval. Such a pacemaker can function quite well provided the atrial stimulus does not interfere with the function of the ventricular channel. If it does, the disturbance is called *AV crosstalk* because the atrial stimulus, if sensed by the ventricular channel, can cause ventricular inhibition.

4.5.7 The fifth fundamental timing cycle

Prevention of crosstalk is mandatory and requires the addition of a brief ventricular blanking period beginning coincidentally with the release of the atrial stimulus. This is known as the *Postatrial Ventricular Blanking (PAVB)* period. No signal can be detected during this blanking period. The ventricular channel “opens” after this short blanking period so that ventricular sensing (with reset of the atrial escape interval and lower rate interval) can occur during the remainder of the AV delay.

The addition of this important blanking interval yields a DDD pacemaker with five basic cycles and two derived cycles. This format was the basis of first generation DDD pacemakers that were clinically used and accepted. Even a sophisticated contemporary DDD pacemaker reduced to having only these seven intervals would function satisfactorily if appropriately programmed. Further addition of timing cycles represents refinements rather than essential elements of DDD pacing.

4.5.8 VSP and Upper Rate Interval programmable independently of the TARP

Further refinements of DDD pacemaker function have introduced two other timing intervals:

1. ventricular safety pacing (VSP) complements the blanking period in dealing with crosstalk – this function does not prevent crosstalk but merely offsets its consequences;
2. upper rate interval programmable independently of the TARP is used to achieve

a smoother upper rate response than the rather abrupt slowing down by the TARP when it is the only interval controlling the upper rate (interval).

Part III

Identification and Documentation of Environmental Assumptions for the PACEMAKER System

Chapter 5

Modeling the PACEMAKER System

The PACEMAKER System is identified as an *embedded, process-control* system, with a specialized medical application. In Section 2.5, the idea of a basic medical instrumentation system was introduced. This generic model is further developed and customized to suit the PACEMAKER System in this chapter in order to capture its operative characteristics and to aid the specification of unambiguous requirements.

Several precise notations have been developed to specify software requirements for embedded, *reactive systems* – among which, the Software Cost Reduction (SCR) notation [15], Statecharts, and the Requirements State Machine Language (RSML) have received considerable attention. The model adopted in this thesis is a variation of Parnas' Four-Variable Model (FVM) [23], which is used in SCR and the version of Parnas' Rational Design Process used in Ontario Power Generation's Safety-Critical

Software Methods [15].

5.1 Definitions and Concepts

Embedded System

Embedded systems are information processing systems that are embedded into enclosing products and that are normally not directly visible to the user.

Controlled Process, Environment, and Control

An embedded system consists of a controller and a controlled, physical part. The term **process** is used to denote the controlled, physical part; and **environment** denotes everything outside the embedded system. Frequently, embedded systems are connected to the physical environment through sensors collecting information about the environment and actuators controlling that environment. The control software is abbreviated to **control** throughout this thesis.

Model

A **model** is a formal representation of the system, e.g., a diagram or a timed automaton. Both the process and the control are modeled and then verified against the required behavior of the system.

In the case of modeling the PACEMAKER System, the derived model is defined by a set of *system boundaries* and associated *interfaces*. The complete model is

introduced and explained in the next section.

5.2 A Formal Model for the PACEMAKER System

This thesis presents a formal model for the PACEMAKER System based on a variation of the Four-Variable Model (FVM) originally defined by Parnas and Madey in [23]. See Figure 5.10 for a depiction of the modified FVM.

5.2.1 The Four-Variable Model

The Four-Variable model is essentially an abstraction of part of the traditional feedback process control model presented in Section 2.5 – in that it specifies relations between the set of *monitored variables* and the set of *controlled variables*. However, it also introduces two new, additional sets of variables – ‘*input*’ and ‘*output*’ variables – which, by specifying their relation, document system design.

The approach to modeling used in SCR [15] is based on this Four-Variable model and, thus, built upon the same classic process control model.

The Four-Variable model enables the documentation of *system requirements*, *system design*, and *software requirements* all at once. Complete behavior of the system is captured and represented formally in terms of four sets of variables – *monitored* (M), *controlled* (C), *input* (I), and *output* (O) variables; and four relations – NAT, REQ, IN, and OUT.

The FVM describes the required behavior of a software system by describing the

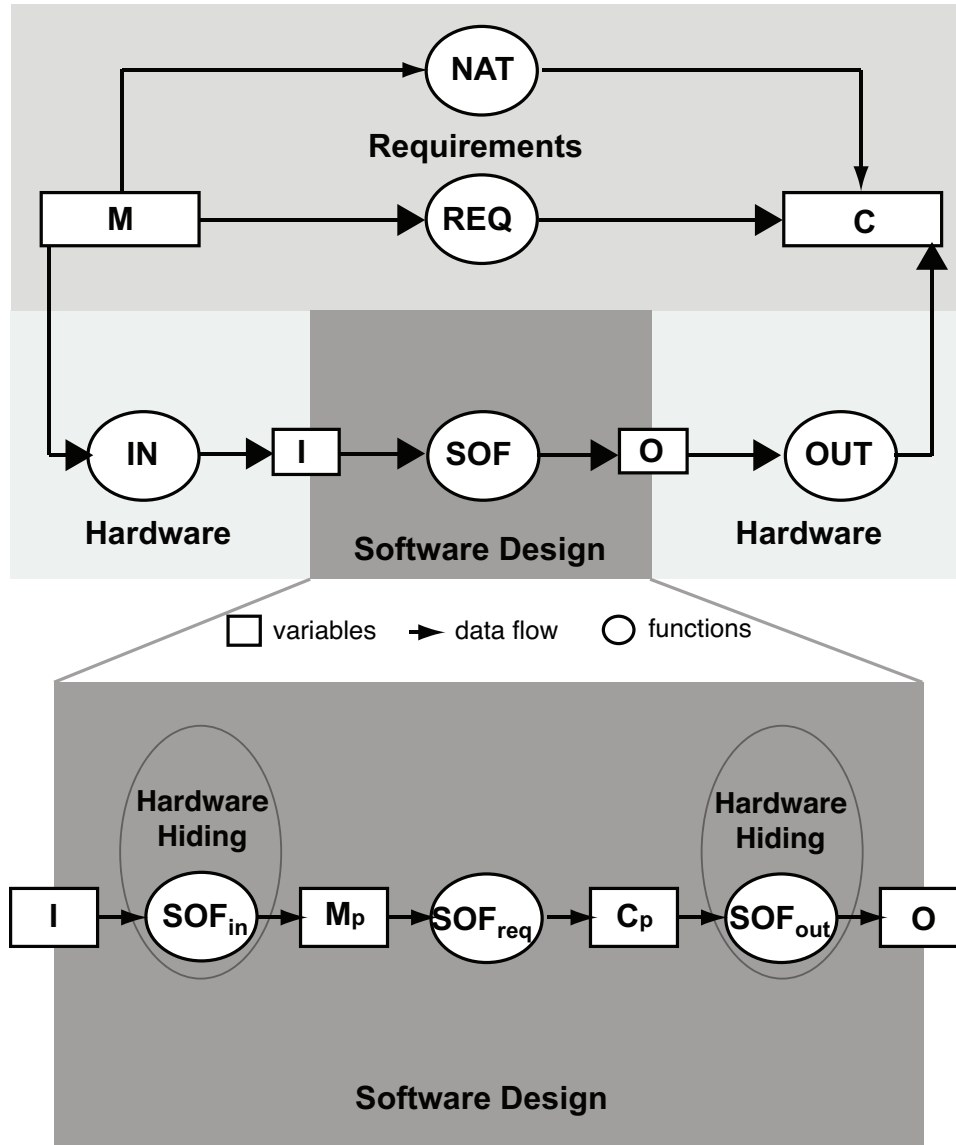


Figure 5.10: The Modified Four Variable Model with Hardware Hiding [23]

required relations between the two sets of time-varying ‘*environmental quantities*’ – the monitored variables and controlled variables. The relation NAT captures constraints on the values of environmental quantities placed by nature and previously installed systems, whereas REQ documents further constraints imposed by the computer system to ensure intended system behavior. In other words, NAT specifies *assumptions* about system behavior restricted by physical laws and the system environment; and REQ describes those aspects of the environment that the system is expected to control – how the system is required to change the controlled quantities in response to changes in the monitored quantities. Thus, the relations REQ and NAT together specify the ‘*black-box*’ behavior of the system.

In contrast, relations IN and OUT are used to specify the behavior of the computer system at the design level, with an emphasis on the peripheral devices. More specifically, at design level, IN describes the behavior of the input hardware by mapping the set of monitored variables to the set of input variables (to the software). Similarly, the connection between output variables and controlled quantities is specified by the relation OUT. In other words, the effects of the system hardware on the input and output variables associated with the software are represented by IN and OUT, respectively.

It is also worth mentioning that neither IN nor OUT is a function, as a result of imprecision in the measurement and transducer devices. This imperfection arising from the hardware introduces great potential among software designers to make assumptions about the system hardware environment. The documentation of these assumptions is vital. Although, in some cases, practitioners have managed to build

software systems correctly without necessarily documenting environmental assumptions they had made during the process – owing solely to their domain expertise – this is a dangerous act. Future modifications may violate some of those unwritten assumptions, and the people involved at that stage of development/maintenance may not have the domain knowledge that the original developers had.

For the PACEMAKER System, a significant proportion of these environmental assumptions are made on the specific system hardware, including the hardware that is directly in contact with the domain environment – the leads; as well as the hardware used as middle-ware between the raw, external signal and the software inputs/outputs – the sensing circuit and output circuit.

In the examination of environmental assumptions for the PACEMAKER System – which is seemingly an activity at the requirements level – it is, however, realized that the software system is highly dependent upon the hardware to interface with its domain environment. Moreover, due to the evolutionary nature of pacemakers, the hardware interface of the PACEMAKER System is well known (e.g. via examining system specifications of a previous generation of the product). Therefore, in this case, it is necessary to include the hardware interface as part of the environment – reflected in the proposed model through the identification of input and output variables, as well as the mappings between M and I, and O and C, which involve the hardware environmental assumptions.

In other words, the identification and documentation of environmental assumptions for the PACEMAKER System are only possible when all of the four relations:

NAT, REQ, IN and OUT, are taken into consideration. That is to say that the construction of a model that resembles the Four Variable Model for the PACEMAKER System is the cornerstone of the elicitation of environmental assumptions.

5.2.2 Modeling the PACEMAKER System

The PACEMAKER System is designed to monitor and regulate a patient's heart rate. At first sight, it seems that a 'traditional' process control model is the perfect candidate for modeling the PACEMAKER System. It seems to provide the right fit – a mapping between the essential components in a generic embedded system and their manifestations in the PACEMAKER System is summarized in Table 5.4. The PACEMAKER pulse generator, in this case, is the controller; it controls, among other things, the amplitude and width of the output electric pulse, and the time intervals between consecutive output pulses. This is what the PACEMAKER system model would look like if a classic process control model had been imposed.

Table 5.4: PACEMAKER system as an process control system

Generic Embedded System	The PACEMAKER System
Controlled process	A patient's heart rate
Environment	The human heart; the cardiovascular system
Control	The Pulse Generator (PG)
Hardware, Output device	Leads

However, the simple model presented in Table 5.4 fails to capture some of a pacemaker's more specific functions – e.g. its interaction with/response to the application of a medical magnet; the pacemaker's corresponding behaviour when the use

of an accelerometer is enabled; and the serial communication the pacemaker's pulse generator has with its external control unit.

In other words, the *domain environment* that the PACEMAKER System finds itself in consists of a number of smaller, mutually exclusive *sub-environments*.

5.2.3 The Domain Environment and Sub-environments

The process of developing a model for the PACEMAKER System – i.e., drawing system boundaries and specifying interfaces at each of these boundaries – is greatly driven by the need for properly identifying environmental assumptions for the system.

Broy proposed in [4] that **Environmental Assumptions** (EAs) be classified as a special kind of Requirements component, namely **Domain analysis**.

“Properties and structures of the application domain. Domain analysis is an important part of requirements engineering, although it does not directly lead to the formulation of requirements but forms its basis. Similar to other documented requirements, the documented properties of the application domain are only an *image* (or a *model*) of the real domain. A thorough analysis is necessary to ensure that this image is sufficiently faithful to reality w.r.t. the system under development. In the context of embedded systems the result of domain analysis is also referred to as the *environment assumptions*. ”

A similar idea was presented again by Leveson in [17]:

“...different types of requirements will affect the design in different ways.

In an intent specification, Level 1 contains three types of “requirements”: functional requirements, environmental assumptions, and design constraints.

Functional requirements are derived from general system goals, i.e., the mission of the system.

Environmental assumptions lead to a second type of requirement that arises as soon as the system boundary is defined and the system interface thus becomes bound to (dependent upon) assumptions about the components in the environment. ”

Domain Environment outside the System

To model the PACEMAKER System, an obvious boundary to draw is a system boundary separating its encompassing physiological environment – one that contains the controlled process – and the system as a whole. However, as was mentioned earlier, the biological environment alone does not fully represent the whole universe of the domain environment for the PACEMAKER System, rather, it is a constituent of it – a sub-environment. Figure 5.11 describes the PACEMAKER System and its four surrounding sub-environments. The first system boundary (**B1**) drawn between the complete PACEMAKER system and its domain environment consists of four sub-boundaries (**B1.1 – B1.4**), specifying:

1. the pacemaker’s interaction with its physiological environment, namely the heart (**B1.1**);

2. the pacemaker's response to the application of a medical magnet (**B1.2**);
3. the pacemaker's corresponding behaviour when the use of an accelerometer is enabled (**B1.3**);
4. the serial communication between the pacemaker's pulse generator and its external control unit (**B1.4**).

B1.1 essentially resembles the one system boundary that is present in the traditional process control model, crossed by a set of monitored variables and a set of controlled variables, which, together, describe the interface between the controlled environment and the controlling system. In the case of the PACEMAKER system, each monitored variable at **B1.1** has a corresponding controlled variable feeding back to the controlled process. This, however, is not true for the interfaces at system boundaries **B1.2 –B1.4**.

See Table 5.5 and Table 5.6 for a summary of the PACEMAKER system interface at **B1.1**.

Table 5.5: Monitored Variables at **B1.1**

Monitored Variables	Type	Description
m_v_amp	mV	Amplitude of unfiltered ventricular signal
m_a_amp	mV	Amplitude of unfiltered atrial signal

Interfaces at each of **B1.2 –B1.4** can be represented in a similar fashion via specifying a corresponding monitored variable (as indicated in Figure 5.11 and Table 5.7)

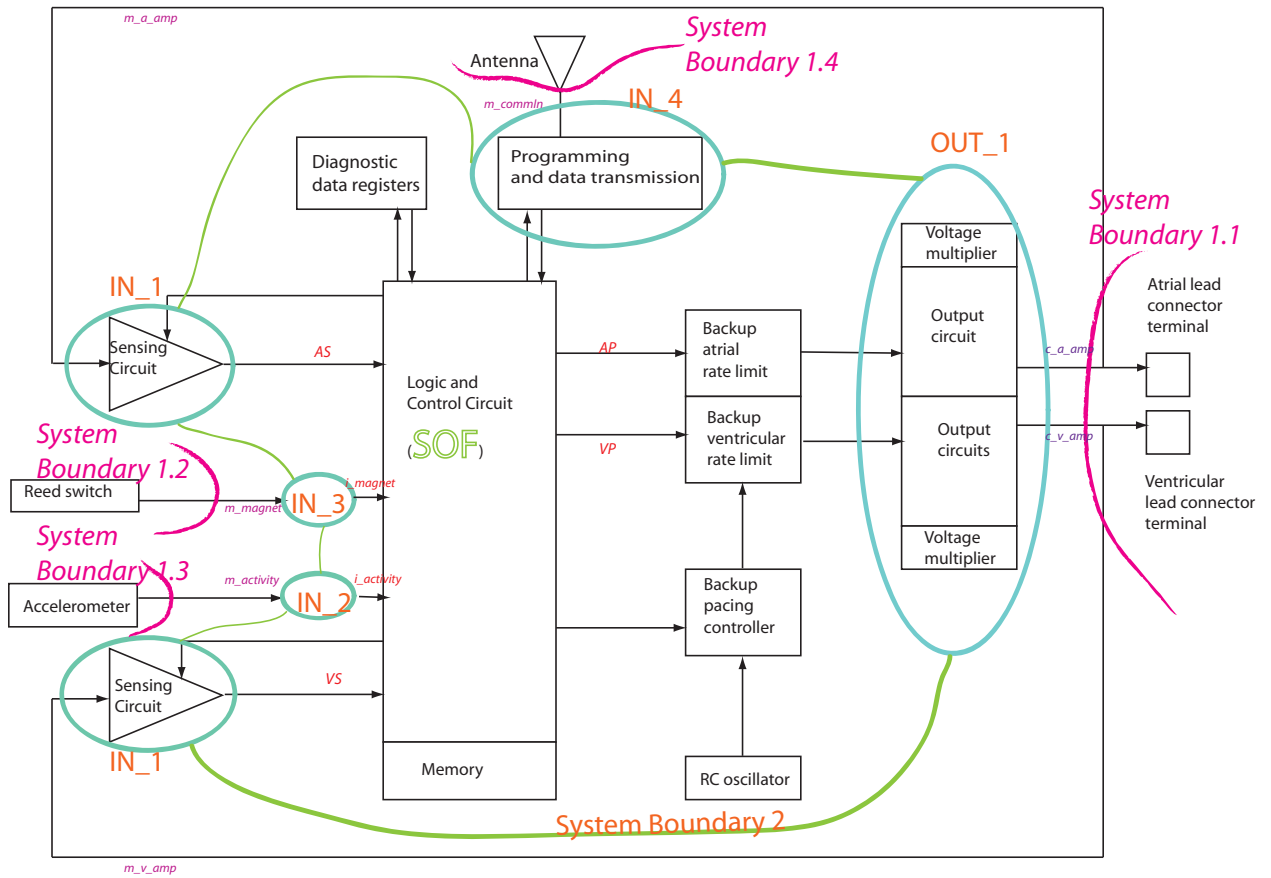


Figure 5.11: Proposed System Structure and System Boundaries

Table 5.6: Controlled Variables at **B1.1**

Controlled Variables	Type	Description
c_v_amp	mV	Amplitude of ventricular pacing signal
c_a_amp	mV	Amplitude of atrial pacing signal

Table 5.7: Monitored Variables at **B1.2** – **B1.4**

Monitored Variables	Type	Description
m_magnet	boolean	The presence of a magnet
m_activity	boolean	True indicates that the lowest level of sensor activation required to initiate an increase in heart rate has been reached.
m_commIn	20-bit binary code	The microprocessor-based transmitter/receiver pair operates by inductively coupling pulse-position modulated, binary coded data from the programmer to the PG.

Hardware Environment within the System

One advantage provided by modeling the PACEMAKER System using the 4-Variable Model is that it allows the incorporation of hardware assumptions by drawing an extra system boundary between the monitored variables, M, and the input variables, I; and, similarly, between O and C. This makes the documentation of assumptions associated with the particular hardware platform – sensing and output circuits – possible. Therefore, a second system boundary is drawn between M and I, or O and C, depending on the direction of data/information flow.

Figure 5.11 includes a depiction of the hardware environment.

One point worth mentioning is that the relation IN has no altering effect on the monitored variables crossing **B1.2** – **B1.4**. In other words, IN is a reflexive relation on $m2$, where $m2 \in \{m_magnet, m_activity, m_commIn\}$.

Also, an unconventional notion is introduced (in modeling the pacemaker's ECG

signals) that deviates from the traditional belief that, in a FVM, the number of input variables always matches the number of monitored variables. As indicated in Figure 5.11, the set of input variables resulting from the sensing circuit has four elements, including two input variables – `raw_v_amp` and `raw_a_amp` – representing the ‘unchanged’, raw signals feeding into the PG.

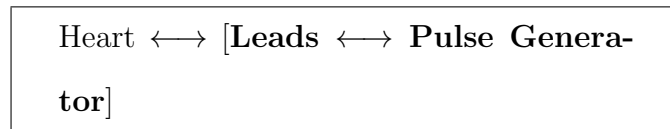
5.2.4 The PACEMAKER Model – System Boundaries and Interfaces

The model used in this thesis to identify environmental assumptions for the PACEMAKER System is presented in this section.

System Boundary 1 in: Domain Environment \longleftrightarrow ‘Complete’ System

Domain Environment is defined as the union of the following four *sub-environments*:

1. The **heart** (physiological); whose signals are sensed by the implanted leads.



2. **Ambient magnetic field** (electro-magnetic); whose presence is detected by the reed switch inside the Pulse Generator.

Magnet \longleftrightarrow (Reed Switch \longleftrightarrow) **Pulse Generator**

3. **A ‘virtual’ environment** specific to rate-adaptive pacemakers; signals generated in this sub-environment are changes in certain monitored physiological parameters of the body. A sensor is used to convert a physiological variable in the patient to an electrical signal that serves as an input to the controller circuitry. Each of the physiological variables requires a different control algorithm for the control circuitry.

The most common sensor is the activity sensor which uses *piezo-electric* materials to detect vibrations caused by body movement.

Δ Body activity \longleftrightarrow the Accelerometer
 \longleftrightarrow **Pulse Generator (circuit board)**

4. **A serial communication channel realized through an information-bearing medium** (usually electro-magnetic); whose presence is detected either by an antenna or the reed switch inside the Pulse Generator.

The external unit generates programmed stimuli which are transferred to the Pulse Generator by one of several communication techniques. See Figure 5.12 for a functional block diagram of the programming interface.

The commonly used methods of transmitting information are:

- (a) **magnetic** – an electromagnet placed on the surface of the body establishes a magnetic field which penetrates the skin and operates the PG’s reed switch;

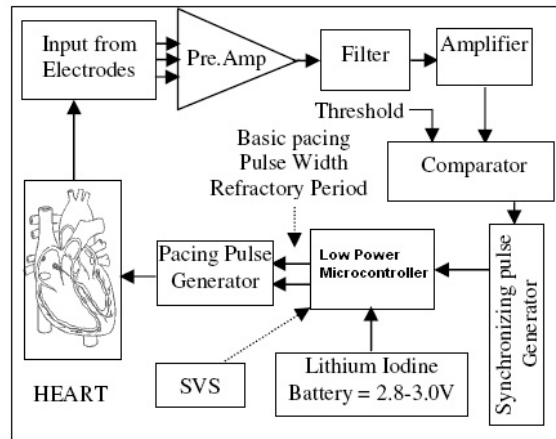


Figure 5.12: A Functional Block Diagram of the Programming Interface between PG and the Control Unit [16]

- (b) **radio-frequency waves** – the information can be transmitted over high frequency electromagnetic waves which are received inside the body by an antenna;
- (c) **acoustic-ultrasonic pressure waves** from a suitable transducer placed over the skin, can penetrate the body. They are received by a suitable receiver in the pacemaker which carries out the desired function.

Out of all these methods, the magnetic field method is the most widely used because of its simplicity and minimal power requirement.

Pulsating electro-magnet \longleftrightarrow (Reed Switch or Antenna \longleftrightarrow) **Pulse Generator**

Complete System consists of:

Leads (as sensors) → Pulse Generator → Leads (as actuators)

Pulse Generator consists of:

... → Sensing Circuit → **Logic, Control and Timing** → Output Circuit →
...

Interface 1: Domain Environment-System Interface (defined in terms of *Monitored Variables*):

M: A set of Monitored Variables.

M_1 : A subset of monitored variables, specifically from sub-environment 1 – the heart.

M_2 : A subset of monitored variables, specifically from sub-environment 2 – the magnet.

M_3 : A subset of monitored variables, specifically from sub-environment 3 – the activity sensor/indicator.

M_4 : A subset of monitored variables, specifically from sub-environment 4 – the serial communication channel.

$$M = M_1 \cup M_2 \cup M_3 \cup M_4 \quad (5.1)$$

$$M_1 = \{m_v_amp, m_a_amp\} \quad (5.2)$$

$$M_2 = \{m_magnet\} \quad (5.3)$$

$$M_3 = \{m_activity\} \quad (5.4)$$

$$M_4 = \{m_commIn\} \quad (5.5)$$

Table 5.8: Monitored Variables

Monitored Variables	Type	Description
m_v_amp	mV	Amplitude of unfiltered ventricular signal.
m_a_amp	mV	Amplitude of unfiltered atrial signal.
m_magnet	boolean	The presence of a magnet.
m_activity	boolean	True indicates that the lowest level of sensor activation required to initiate an increase in heart rate has been reached.
m_commIn	20-bit binary code	The microprocessor-based transmitter/receiver pair operates by inductively coupling pulse-position modulated, binary coded data from the programmer to the Pulse Generator.

System Boundary 2_in: Input Hardware/pre-SOF

processing: $M \longleftrightarrow \text{Input Hardware} \longleftrightarrow I$

$M \longrightarrow \text{System Input Hardware} \longrightarrow I$

M: Monitored variables from Interface 1 – raw/unfiltered, analogue heart signals from the leads (atrial or ventricular); magnetic waves from the magnet; electromagnetic waves from the communication unit; and body motion.

I: Input variables to the software – hardware-processed (filtered and level-selected) signals (modeled as event markers, e.g., VS, AS.)

Interface 2: Hardware-Software Interface (defined in terms of *Input Variables*)

See Table 5.9 for a list of input variables.

Table 5.9: Input Variables

Input Variables	Type	Description
AS	boolean	Atrial Sense
VS	boolean	Ventricular Sense
raw_a_amp	mV	Raw, unchanged atrial signal, feeding into EG (e-graph)
raw_v_amp	mV	Raw, unchanged ventricular signal, feeding into EG (e-graph)

System Boundary 2_out: $O \longleftrightarrow$ Output Hardware

$\longleftrightarrow C$

$O \longrightarrow \text{Output Circuit} \longrightarrow C$

O: Output variables from the software component.

C: Controlled variables. Output electrical pulses/stimuli for the heart. See Table 5.9.

Interface 3: Software-Output Hardware Interface (defined in terms of *Output Variables*)

See Table 5.10 for a list of output variables.

Table 5.10: Output Variables

Output Variables	Type	Description
AP	boolean	Atrial Pace
VP	boolean	Ventricular Pace

System Boundary 1_out: System \longleftrightarrow Domain Environment

$C \longrightarrow \text{Leads} \longrightarrow \text{Heart}$

Interface 4: (defined in terms of *Controlled Variables*)

See Table 5.11 for a list of controlled variables.

Table 5.11: Controlled Variables

Controlled Variables	Type	Description
c.v.amp	mV	Amplitude of ventricular pacing signal
c.a.amp	mV	Amplitude of atrial pacing signal

Chapter 6

Environmental Assumptions at System Boundary B1.1 for the PACEMAKER Model

Figure 5.11 from the previous chapter describes the PACEMAKER System and divides its domain environment into four sub-domains – the biological, the communication, the magnet, and the accelerometer sub-domains.

These four sub-domains, although sharing the same system boundary, are very different, and so are the environmental assumptions associated with each. Moreover, not all of the four sub-domains are particular to the PACEMAKER problem. For instance, the sub-domain representing the serial communication is not native to the pacemaker. It can be considered as an independent problem, concerning communication protocol design, data verification and transmission, noise filtering, etc.

Furthermore, the complexity of such a communication problem is typically profound – so profound that to identify environmental assumptions in this sub-domain would require an enormous volume of documentation, thus becoming a daunting problem that is better dealt with separately.

Since the research presented in this thesis originated with an inclination/direction towards exploring the biological side of the PACEMAKER problem, the main focus of this thesis is to identify and present the environmental assumptions concerning system boundary **B1.1**, i.e. those environmental assumptions made within the biological sub-domain.

In addition, study of one of **B1.2** and **B1.3** is chosen to demonstrate the documentation of environmental assumptions from a different sub-domain. It is considered a similar type of problem as that imposed by **B1.4**, only of a smaller size.

This chapter deals with the identification and documentation of environmental assumptions concerning system boundary **B1.1** for the PACEMAKER. It discusses the process that was used for the assumptions' elicitation, as well as for their refinement; it also proposes a documentation convention/format in order to further specify the characteristic (type), significance, and relevance of each of the environmental assumptions identified.

6.1 Identifying Environmental Assumptions Concerning System Boundary 1.1: Heart \longleftrightarrow Complete System

Heart \longleftrightarrow [Leads \longleftrightarrow Pulse Generator]

Chapter 2 presented a list of general constraints in the design of medical instrumentation systems, including:

- Variability of Physiological Parameters
- Interference among Physiological Systems
- Sensor Interface Problems
- High Possibility of Artifacts
- Safe Levels of Applied Energy

This generic list of constraints is used as a guideline in this and the next chapter to aid the elicitation of environmental assumptions for the PACEMAKER system.

Each clause in the above list is applied to the PACEMAKER system, and a list of environmental assumptions specific to the PACEMAKER system is generated under each heading.

Other ideas presented in Chapter 2 and 3, such as the characteristics of various biosignals and the functional behaviour of the cardiovascular system, are also reflected in the elicitation, classification and organization of the PACEMAKER's environmental assumptions.

6.2 Refinement of the Elicited Environmental Assumptions

The above described elicitation process – using the list of constraints for general medical instrumentation systems as a guide – produces a set of environmental assumptions for the PACEMAKER system concerning the biological interface. However, the resultant set of environmental assumptions may contain assumptions that are either too descriptive/qualitative or irrelevant to the clarification of the original PACEMAKER System Specification. Therefore, the initial list of the environmental assumptions obtained requires further refinement.

The refinement process proposed in this thesis starts with looking at each of the elicited assumptions individually and asking the following three questions:

1. What – What kind of assumption is it? The type of assumption defines whether an assumption is *definitive*, *descriptive*, or *quantitative*.
2. Why – Why it is important/necessary to document this assumption? What is its significance in terms of aiding system requirements specification, design documentation, future system upgrades, and maintenance?

3. How – How is it related to the original PACEMAKER System Specification?

In what respect does the assumption help to clarify the original requirements document? It also asks how it is related to the behavioural assumptions identified for the PACEMAKER system in Chapter 8, or the system’s hardware assumptions documented in Chapter 7.

6.2.1 The Type of Assumptions

It is important to identify the type of the assumption under consideration, as knowing the nature of each of the assumptions, i.e., which category it belongs to, will allow the classification of the environmental assumptions identified, thus in turn enabling better documentation and easier referencing in the future.

The type of environmental assumptions identified for the PACEMAKER system at system boundary B1.1 fall into the following four general types:

Definitive: this type of assumption is essentially a missing definition on a vague term in the original PACEMAKER System Specification. It helps clarify the meaning of clauses in the original document, enhances its readability, and clears off some of the domain knowledge related barriers for the reader of the original PACEMAKER System Specification.

Necessary domain knowledge, descriptive: this type of assumption states domain-knowledge-related necessary conditions for the proper/correct functioning of the PACEMAKER system. Examples from this category include assumptions

resulting from the requirements for effective pumping of the heart and assumptions on the cardiac cycle.

Necessary domain knowledge, quantitative: this type of assumption documents necessary, quantitative domain knowledge in a precise manner with specific numerical values. Because of its quantitative nature, this type of environmental assumption is easily verified; these assumptions put constraints directly on the design decisions system engineers have to make. Examples from this category include the assumptions made on the range of the bioelectric signal, assumptions on the normal human heart rate at rest, and the various firing rates of natural pacemakers.

PACEMAKER hardware design assumption, descriptive: this type of assumption specifies hardware-related domain knowledge or requirements that affect the PACEMAKER system's hardware design. For example, special properties of the bipolar system that make it more favourable than the unipolar system are environmental assumptions of this type.

PACEMAKER hardware design assumption, quantitative: this type of assumption specifies implied knowledge or requirements on the hardware design of the PACEMAKER system. For example, the safe levels of energy the PACEMAKER is applying to the heart is an environmental assumption of this type.

6.2.2 Classification and Organization of the Assumptions – Documentation Convention

The documentation system used in this thesis for the environmental assumptions follows the following convention, where each assumption identified is discussed in three aspects:

1. **Type** – What kind of assumption it is.
2. **Significance** – Why it is necessary to document this assumption; what difference would it make not to include this assumption in the documentation.
3. **Relevance** – Its relevance to the original PACEMAKER System Specification, i.e., how does it help to clarify the original document; as well as its relevance to other chapters in the thesis, for example, the system behavioural assumptions documented in Chapter 8 (Assumptions Concerning System Behaviour), or the system hardware assumptions documented in Chapter 7. It is also worth mentioning that environmental assumptions that are ‘entirely’ missing from the original PACEMAKER System Specification are also identified, possessing no direct relevance to clauses in any of the existing documents. In such a case, the label ‘*independent missing assumption*’ is used as an indicator for assumptions that fall into this category.

6.3 Aspects of NAT governed by the Cardiovascular System

6.3.1 Characteristics of the Biosignal

1. The biosignals sensed by the PACEMAKER system are the bioelectric signals produced by the heart.

Type: Necessary domain knowledge, descriptive.

Significance: This assumption specifies the type of biosignals the PACEMAKER is expected to handle. It imposes implied constraints on the design decisions made on the PACEMAKER hardware – the sensing circuit, for example – and the type of sensors the PACEMAKER system ought to employ.

Relevance: (a) To *Chapter 8 System Behaviour Assumptions* – This assumption provides the foundation/base of the behavioural assumptions documented in Chapter 8. The characteristics and behaviour that the PACEMAKER system implementation has to comply with are defined by this premise, i.e., that ‘the biosignal is the bioelectric signals produced by the heart’.

(b) To *the PACEMAKER System Specification* – Section 3.4 - 3.6, Section 4, Diagnostics, and Section 5, Bradycardia Therapy. In general, this assumption provides fundamental reasoning for the system requirements documented in Sections 3, 4, and 5. Detailed assumptions

associated with each of the requirements in these three sections are presented in the later sections in this chapter.

2. The sensed signal to the PACEMAKER is the voltage or potential difference between the two intracardiac electrodes.

Type: Definitive.

Significance: This assumption answers the question ‘what does the pacemaker sense’?. In other words, it defines the characteristics of the input signal to the PACEMAKER by specifying how it is measured.

Relevance: (a) To *the PACEMAKER System Specification* – Section 3.4.4, Sensitivity Adjustment. Section 3.4.4 specifies the need for the PACEMAKER to have a pre-settable sensitivity level (or sensing threshold) for both the ventricular and atrial sense channels. This sensing threshold is reflected in Appendix A, Programmable Parameters, as an incremental Voltage value - ‘A or V Sensitivity’.

Also, to Section 3.3 Lead Support - the characteristic of the system’s sensed signal determines the selection choice of the sensor, in this case the leads.

(b) To *Chapter 7 System Hardware Assumptions* – the relevance of this assumption to Section 3.3 on lead support is once again repeated in more detailed fashion in Chapter 7, where hardware assumptions on the PACEMAKER system’s sensor are discussed in more depth.

3. Normal human heart rate at rest is assumed to be 60–90 beats/min.

Type: Necessary domain knowledge, quantitative.

Significance: This is a typical environmental assumption posed by the natural biological environment the system is interacting with, or NAT. It specifies the range of the naturally occurring biosignal the PACEMAKER is supposed to deal with. In addition, it defines what range of the input signals are considered as ‘normal’ signals, expressed in term of heartbeats per minute. This assumption serves as the base for the next assumption, where the range of valid signals accepted by the PACEMAKER system is specified.

Relevance: (a) To *the PACEMAKER System Specification* – In Appendix A, nominal values of the Lower Rate Limit, Upper Rate Limit, and the Maximum Sensor Rate are specified. These numerical values are determined according to the naturally occurring normal range of input signals stated in this particular environmental assumption.

4. The frequency range of the bioelectric signal is assumed to be 25–300 beats per minute.

Type: Necessary domain knowledge, quantitative.

Significance: This environmental assumption states the range of valid input signals. It is a direct result of the previous (3.) assumption. It is necessary because it delineates the system scope in terms of the validity of input governed by the natural laws of physiology, or NAT (60–90 beats/min), with some degree of fault tolerance (25–300 beats/minute vs.

60–90 beats/min). With this assumption, the system hardware designers are obliged to design system hardware to only let endocardial signals with the right frequency content into the system without attenuation; and the system software designers will, therefore, be able to focus their attention on only dealing with the valid range of inputs, all other signals would have been viewed as invalid inputs and filtered out previously. Such an arrangement is usually achieved through the employment of a band-pass filter in the pacemaker’s sensing circuit. More filter-related, specific assumptions are documented in the next Chapter - *System Hardware Assumptions*.

- Relevance:** (a) To *the PACEMAKER System Specification* – Section 5.1 Lower Rate Limit (LRL) and Section 5.2 Upper Rate Limit (URL).
(b) To *Chapter 8 System Behaviour Assumptions* – Section 8.1.3 Lower Rate Limit/Interval (LRI) and Section 8.1.6 Upper Rate Interval (URI).

6.3.2 Characteristics of Natural Cardiac Pacemakers

1. Firing rate of the heart’s primary pacemaker (SA node) is 60–100 per minute.

Type: Necessary domain knowledge, quantitative.

Significance: Closely related to assumption 3.1.3 (Section 6.3.1, assumption 3), this assumption further specifies the rationale behind the requirements on LRL (35-50ppm; 50-90ppm; 90-175ppm, with a nominal value of 60ppm) and URL (50-175ppm, with a nominal value of 120ppm) by

stating the normal range of firing rate of the heart's primary pacemaker;
thus further stating the restraint posed by the physiological environment.

Relevance: (a) To *the PACEMAKER System Specification* – Section 5.1
Lower Rate Limit (LRL) and Section 5.2 Upper Rate Limit (URL).

(b) To *Chapter 8 System Behaviour Assumptions* – Section 8.1.3 Lower
Rate Limit/Interval (LRI) and Section 8.1.6 Upper Rate Interval
(URI).

2. Firing rate of the heart's secondary pacemaker (AV node) is 40–60 per minute.

Type: Necessary domain knowledge, quantitative.

Significance: Closely related to assumption 3.1.3 (Section 6.3.1, assumption 3), this assumption further specifies the rationale behind the requirements on LRL (35-50ppm; 50-90ppm; 90-175ppm, with a nominal value of 60ppm) and URL (50-175ppm, with a nominal value of 120ppm) by stating the normal range of firing rate of the heart's secondary pacemaker; thus further states the constraint posed by the physiological environment.

Relevance: (a) To *the PACEMAKER System Specification* – Section 5.1
Lower Rate Limit (LRL) and Section 5.2 Upper Rate Limit (URL).

(b) To *Chapter 8 System Behaviour Assumptions* – Section 8.1.3 Lower
Rate Limit/Interval (LRI) and Section 8.1.6 Upper Rate Interval
(URI).

3. Firing rate of the heart's tertiary pacemaker is 20–40 per minute.

Type: Necessary domain knowledge, quantitative.

Significance: Closely related to assumption 3.1.3 (Section 6.3.1, assumption 3), this assumption further specifies the rationale behind the requirements on LRL (35-50ppm; 50-90ppm; 90-175ppm, with a nominal value of 60ppm) and URL (50-175ppm, with a nominal value of 120ppm) by stating the normal range of firing rate of the heart's tertiary pacemaker; thus further states the constraint posed by the physiological environment.

Relevance: (a) To *the PACEMAKER System Specification* – Section 5.1 Lower Rate Limit (LRL) and Section 5.2 Upper Rate Limit (URL).
(b) To *Chapter 8 System Behaviour Assumptions* – Section 8.1.3 Lower Rate Limit/Interval (LRI) and Section 8.1.6 Upper Rate Interval (URI).

6.3.3 Interference among Physiological Systems

1. The unfiltered sensed signals coming into the system from sub-environment 1 – the physiological environment – may contain undesirable signals, some of which originates from external sources:
 - (a) myopotentials from skeletal muscles (external)
 - (b) electromagnetic interference (external)
 - (c) T waves (internal, but undesirable)

Type: Necessary domain knowledge, descriptive.

Significance: This assumption documents the interference experienced by the PACEMAKER system from external sources. It provides a spectrum analysis of the constituents of the raw, sensed incoming signal. This assumption is important because it provides a base for the system's hardware design rationale (i.e., the filter design in the sensing circuit) – that only heart signals with the right frequency content are allowed to pass into the system without attenuation; signals with a high frequency that originate from an external source should be strongly attenuated so that they no longer can affect the timer; signals with a very low frequency content corresponding with T waves are also strongly attenuated and unable to affect the timer of the pacemaker.

Relevance: (a) To *Chapter 7 System Hardware Assumptions* – Section 7.2.2 Band-Pass Filter.

6.3.4 Safe Levels of Applied Energy

The voltage of a permanent pacemaker refers to the amplitude of the leading edge, which is always constant.

1. The voltage of the PACEMAKER is close to 5.4 V.

Type: PACEMAKER hardware design assumption, quantitative.

Significance: This assumption documents the applied electric pulse of the PACEMAKER to the heart. The value 5.4 V is pre-determined by the

fact that the lithium iodine cell used by the PACEMAKER generates a voltage of 2.8 V which is then doubled electronically.

Relevance: (a) To the *PACEMAKER System Specification* – Section 3.4 Pacing Pulse.

2. The pacemaker stimulus charges the electrode-tissue interface to the *polarization voltage*, which is subsequently dissipated over a period much longer than the brief pacemaker stimulus, creating the ‘*afterpotential*’.

Type: Necessary domain knowledge, descriptive.

Significance: This assumption documents an important concept of ‘afterpotential’. Afterpotential can play a role in problems associated with oversensing, i.e. unintended sensing of certain events.

Relevance: (a) To *Chapter 7 System Hardware Assumptions* – Section 7.2.2 Band-Pass Filter.

3. The pacing threshold is the minimum electrical activity – determined in terms of volts (V) and pulse duration – that causes consistent pacing outside the myocardial refractory period of the heart.

Type: Definitive.

Significance: This assumption documents the definition of the ‘pacing threshold’, which is an important notion when it comes to determining the safety margin of the PACEMAKER’s output voltage. Every effort should be made at the time of implantation to obtain a pacing threshold as low

as possible because its initial value may ultimately determine the threshold at maturity and hence the voltage and pulse duration required for safe long-term pacing. Therefore, a firm grasp on the concept of pacing threshold is the key to the understanding of the PACEMAKER's safety margin, which is documented in the next assumption.

Relevance: (a) To the *PACEMAKER System Specification* – Section 4.5 Threshold Test.

4. The general recommendation is a voltage safety margin of 2 (or 100%), i.e., the output voltage of the pacemaker should be double the chronic voltage threshold at the same pulse duration. Voltage safety margin = output voltage / threshold voltage = 2:1 at an identical pulse duration.

Type: Necessary domain knowledge, descriptive; definitive.

Significance: This assumption documents the safe levels of applied energy specific to the PACEMAKER system. It prescribes a nominal, universally accepted value for the safety margin. Usually, the output voltage and pulse duration of the pacemaker are programmed 8 weeks after implantation to maintain consistent long-term capture with an adequate margin of safety and maximal conservation of battery capacity. However, due to the fact that the capture threshold can vary during the course of a normal day and according to metabolic and pharmacological factors, it is important to provide protection for threshold fluctuation by a safety margin in terms of the pacemaker output. This particular assumption's

significance lies within the fact that it formally defines the safety margin for the PACEMAKER, and provides a value that is prevalently used in practice.

Relevance: Additional to the *PACEMAKER System Specification*.

6.4 Assumptions Concerning Ventricular/Atrial Stimulation

6.4.1 Assumptions concerning refractory periods

1. The *myocardial refractory period* refers to stimulation, i.e., ventricular capture, whereas the *pacemaker refractory period* refers to the sensing function of the device.

Type: Definitive.

Significance: This assumption distinguishes between the two ‘refractory periods’. While *pacemaker refractory period* is used (both in Chapter 8 and the original *PACEMAKER System Specification*) to specify the proper behaviour of the PACEMAKER system, myocardial refractory period is a term used in describing the related biological environment, thus helping explain why certain behaviour of the PACEMAKER – for example, the demand of extra timing cycles such as the Ventricular Refractory Period (VRP) – is indeed necessary. Furthermore, this assumption clarifies any potential confusion that might have been caused by the usage of vague

terminology in the original *PACEMAKER System Specification*, where the term ‘refractory period’ is loosely used without further specifying which of the above mentioned refractory periods it is referring to. It is assumed (the only one that makes sense is) that the term ‘refractory period’ in the original *PACEMAKER System Specification* refers to the ‘pacemaker refractory period’.

Relevance: (a) To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

2. The ventricular myocardial refractory period consists of an *absolute refractory period* and a *relative refractory period*.

Type: Definitive.

Significance: This assumption further documents the definition of a myocardial refractory period, which is an important notion in predicting the response (or capture) of the heart when stimulus from the PACEMAKER is applied. It is used in the assumptions followed to further specify the precise behaviour/feedback of the environment (human heart) the PACEMAKER is trying to control.

Relevance: (a) To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

3. No stimulus can activate the ventricle during the absolute refractory period.

Type: Necessary domain knowledge, descriptive.

Significance: This environmental assumption documents the response of the heart when a stimulus from the PACEMAKER is applied during the absolute refractory period. It provides the reason for the need of a VRP in the timing cycle design of the PACEMAKER. It also explains why a stimulus in the absolute ventricular refractory period is ineffectual.

Relevance: (a) To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

4. Only a stronger than normal stimulus can activate the ventricle during the relative refractory period.

Type: Necessary domain knowledge, descriptive.

Significance: This environmental assumption documents the response of the heart when stimulus from the PACEMAKER is applied during the relative refractory period. It provides a suggestion among other possible causes for the rarely-occurring, undesirable responses of the heart, such as crosstalk, while the PACEMAKER is at work. This assumption also serves as the fundamental justification of the need for a ventricular blanking period in the timing cycle design of the PACEMAKER.

Relevance: (a) To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

5. A normal stimulus outside of the myocardial refractory period activates the ventricular myocardium.

Type: Necessary domain knowledge, descriptive.

Significance: This environmental assumption documents the response of the heart where a normal capture is expected. It specifies the time period during which a stimulus from the PACEMAKER is effective.

Relevance: (a) To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

Chapter 7

Assumptions on System Hardware

(B2)

The identification of a second system boundary (**B2**) allows the documentation of another type of environmental assumptions – the assumptions made on the system’s hardware. More specifically, ‘hardware’ in the PACEMAKER system refers to the circuitry inside the pulse generator. In other words, it is the layer between the monitored variables coming from the external environment and the input variables feeding into the system’s software. This chapter also discusses the environmental assumptions made on the leads, which perform a dual role as both the sensor and the actuator in the PACEMAKER system.

The environment in which the system and software are operating will change over time, partially as a result of increases in system sophistication and performance

optimization. Basic assumptions made about the original hardware platform (environment) must be documented and then periodically evaluated to ensure that they are not being violated in practice. Assumptions made on the characteristics and functional behaviour of the electrodes and the circuitry inside the pulse generator shall be documented as part of the design documents. This chapter provides an example of the documentation of such assumptions.

7.1 An Extension to the Proposed Documentation Convention

A study of great designers found that one attribute they had in common was their ability to anticipate change [11]. Accommodating changes is one of the most challenging aspects of good software design. The goal is to isolate unstable areas so that the effect of a change will be limited to one routine, class, or package. McConnell [18] identifies a series of steps one should follow in preparing for such perturbations:

1. Identify items that seem likely to change.
2. Separate items that are likely to change – achieved via *abstraction*.
3. Isolate items that seem likely to change – achieved via *encapsulation*.

The common areas that are likely to change in a software system include business rules, hardware dependencies, input and output, nonstandard languages features, and difficult design and construction areas. Among these, *hardware dependencies* is the

most relevant to the PACEMAKER project, and should be documented as part of the requirements specification as assumptions.

The proposed documentation convention for environmental assumptions – the one that is used throughout the previous chapter – is extended in this chapter to include a new element, storing the likelihood-of-change index for each of the hardware assumptions identified.

For example, information associated with a typical hardware assumption would be documented using the following format after its identification.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: ...

Relevance: Independent missing assumption.

Likelihood of Change: *Likely*.

7.1.1 Likelihood of Change Index

For the purpose of illustration, this thesis defines two levels of likelihood-of-change:

Likely: the identified hardware assumption is highly likely to change within 12 months;

Not likely: the identified hardware assumption is not likely to change within 12 months.

For a further discussion on the use of the *Likelihood of Change Index*, please see the Future Work section in Chapter 11.

7.2 Environmental Assumptions Concerning the Leads

In Section 3.3, Lead Support, of the original *PACEMAKER System Specification* (see pages 15-16 of [25]), specification of the type of lead supported by the system is given as follows:

1. The Atrial Bipolar Pace/Sensing lead system type shall be supported.
2. The Ventricular Bipolar Pace/Sensing lead system type shall be supported.
3. The system shall operate normally with atrial pace/sense leads between 100 and 2500 ohms.
4. The system shall operate normally with ventricular pace/sense leads between 100 and 2500 ohms.

Unless the audience has some related medical or signal processing background, questions may arise. For example, it is not clear as to what the specification means by ‘bipolar’, nor the reason behind the choice of such impedance ranges – 100 to 2500 ohms. In addition, there is a gap between the particular hardware choices documented in the original system specification and their corresponding software implications, i.e., how would potential changes in the hardware configuration affects the system’s software in the foreseeable future?

Clearly, certain definitions and assumptions are missing. In this section, hardware assumptions on the leads used in the PACEMAKER are elicited with the intention

of aiding the comprehension of the original system specification and easing the adaptation process of the current system to future changes in the hardware.

7.2.1 Assumptions Concerning Bipolar Leads

1. In the bipolar system, both electrodes are approximately of the same size and both are placed inside or on the heart – the current flows between the two electrodes.

Type: Definitive.

Significance: This assumption documents the definition of a bipolar system.

Relevance: (a) To the *PACEMAKER System Specification* – Section 3.3
Lead Support.

Likelihood of Change: Not likely.

2. Bipolar leads by virtue of their greater signal-to-noise ratio allow the use of higher sensitivities.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the special property of bipolar leads that makes them superior to unipolar leads – bipolar leads promote greater protection against extraneous interference. This assumption supports the decision of choosing bipolar leads, documented in the original PACEMAKER System Specification, over unipolar leads for the PACEMAKER system.

Relevance: (a) To the *PACEMAKER System Specification* – Section 3.3
Lead Support.

Likelihood of Change: Not likely.

3. A high sensitivity is especially useful for atrial sensing, an important requirement of contemporary dual chamber pacemakers with the capability of diagnosing supraventricular tachyarrhythmias.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the requirement on sensitivity posed by modern pacemakers, hence placing constraints on the selection of sensing device – in this case, the lead system.

Relevance: (a) To the *PACEMAKER System Specification* – Section 3.3
Lead Support.

Likelihood of Change: Not likely.

4. Bipolar leads are associated with less crosstalk in dual chamber pacemakers.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents another favourable property of bipolar leads – the ability to reduce ventricular sensing of the atrial stimulus.

Relevance: (a) To the *PACEMAKER System Specification* – Section 3.3
Lead Support.

Likelihood of Change: Not likely.

5. Bipolar leads are less sensitive than unipolar systems to external interference (myopotentials, etc.).

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents one of the favourable properties of bipolar leads.

Relevance: (a) To the *PACEMAKER System Specification* – Section 3.3 Lead Support.

Likelihood of Change: Not likely.

7.2.2 Assumptions Concerning the Sensing Electrode Impedance

1. A sensing electrode has certain impedances associated with it. The degree to which sensing impedance affects pacemaker sensing is dependent on the ratio of the input impedance of the sensing amplifier to the sensing impedance. Typically, most pacemakers have an input impedance of 20 k Ω or greater.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the necessary domain knowledge associated with electrode impedance; it thereby explains why a certain range of impedance is suggested in the original PACEMAKER System specification.

Relevance: (a) To the *PACEMAKER System Specification* – Section 3.3
Lead Support, points 3 and 4.

Likelihood of Change: Not likely.

7.3 Environmental Assumptions Concerning the System Hardware Architecture of the PACEMAKER System

As pacing functions have become increasingly complex, it has become standard practice to build circuitry in a more general, computer-based architecture, with functions specified in software. This provides a greater degree of freedom than would be the case for making any changes in hardware, and allows non-invasive modification of software after implantation. The PACEMAKER system is a software-based pacemaker. A typical software-based pacemaker consists of a telemetry system, decoder, timing circuit, analog sensing, and output circuitry. This section documents the environmental assumptions concerning the underlying hardware architecture of the PACEMAKER system. Specific assumptions concerning each constituent component within the structure are explored more comprehensively in the following sections.

7.3.1 System Architecture

1. As a programmable pacemaker, the PACEMAKER is assumed to have a system architecture similar to the one presented in Figure 7.13. It may be considered

as being comprised of three major systems: the *Output Circuit*, the *Sensing Circuit*, and the *Logic and Control Circuit*.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption lays out the underlying system architecture for the PACEMAKER system. It decomposes the PACEMAKER system into three interacting components, each encapsulating a set of related functions. This assumption on the fundamental system architecture and its decomposition for the PACEMAKER system is a cornerstone in the identification process for assumptions on lower system levels, i.e., those assumptions concerning each individual sub-system. It is important because it differentiates the hardware portion of the system – the Output Circuit and the Sensing Circuit – from the software portion – the Logic and Control Circuit, thereby enabling a thorough, yet much clearer, view of the system composition as well as a discussion of the hardware system related environmental assumptions separate from their software counterpart.

Relevance: Independent missing assumption.

Likelihood of Change: Likely.

2. **System 1** – the Output Circuit – controls the main timing functions of the pulse generator and carries the rate limiter, the pulse output circuit and the stimulating function of the electrode. Operating as directed by the Logic and Control Circuit, this system generates output pulses at the programmed rate,

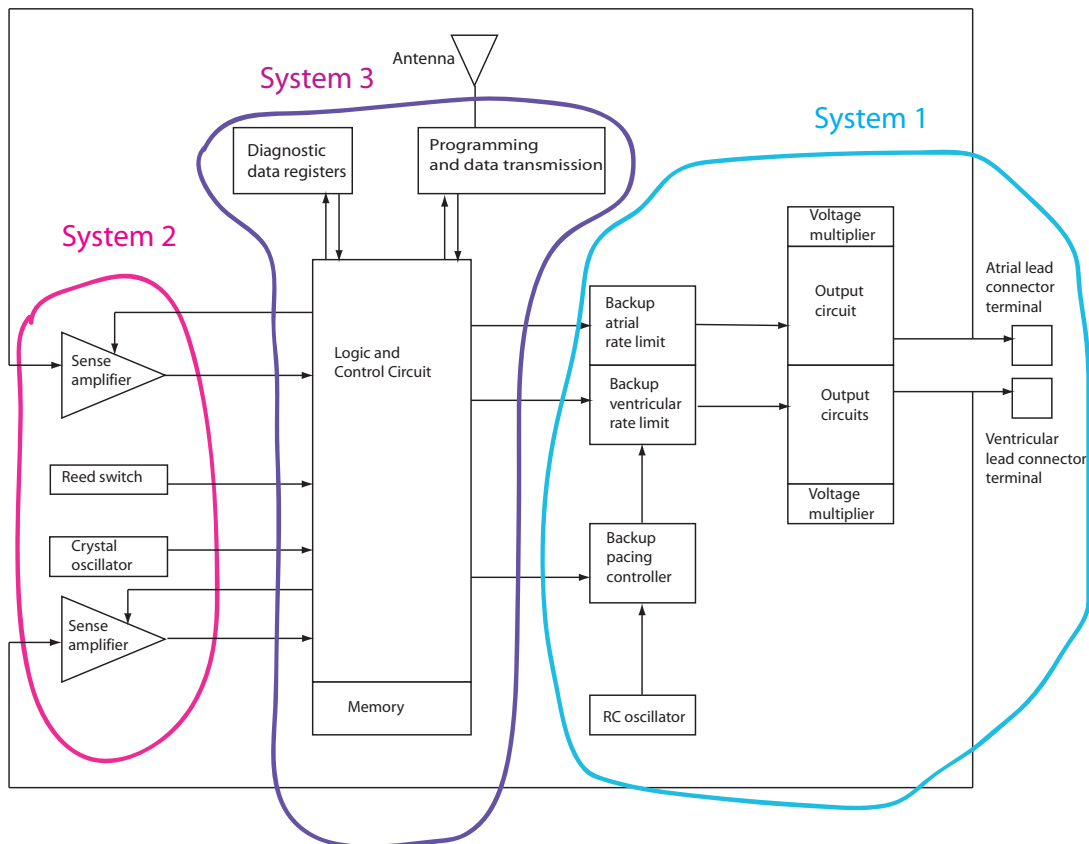


Figure 7.13: Block diagram of a multi-programmable pulse generator.

width and amplitudes unless over-ridden by System 2 when an intrinsic heart signal is sensed.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption outlines the basic functions performed by System 1 – the Output Circuit, and the corresponding components that belong to this particular piece of circuitry. It also characterizes the interfaces through which System 1 interacts/communicates with the rest of the system components. In other words, this assumption documents the relation (in terms of the direction of data flow) between the Output Circuit and the Logic and Control Circuit, as well as the indirect influence of System 2 on the Output Circuit.

Relevance: Independent missing assumption.

Likelihood of Change: Likely.

3. **System 2** – the Sensing Circuit – carries the sensing and signal discriminating function of the circuit. Comprising the sensing function of the electrode, a band-pass filter, a signal amplifier and comparator (i.e., a level detector), this system identifies signals of cardiac origin and, where appropriate, sends an inhibit signal to System 1.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption captures the essential concepts that are the basis of the sensing mechanism used by the PACEMAKER system. Similar to the preceding assumption, this assumption also identifies some of

the subcomponents that constitute the Sensing Circuit, i.e., the band-pass filter, the signal amplifier, and the level detector. This further decomposition of the Sensing Circuit has enabled the elicitation of more hardware related environmental assumptions on an even more refined, subcomponent-wise system level.

Relevance: Independent missing assumption.

Likelihood of Change: Likely.

4. **System 3** – the Logic and Control Circuit – is where the software portion of the PACEMAKER system resides; two kinds of memory are involved: read-only memory (ROM) and random access memory (RAM). Software instructions are stored in ROM, with programmable settings such as pacing rate, pulse amplitude, pulse width, sensing gain, etc. kept in RAM. The ROM circuitry is designed to check for the error-free flow of information, conduct internal self-testing routines during each pacing operation and switch to a back-up pacing system if errors are detected, thus reducing the possibilities of software errors causing anomalous pacing behaviour. Data such as serial number, patient identification and diagnostic information are stored in RAM, along with more complex features.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption, by setting out its software-centric characteristic, classifies the PACEMAKER as an embedded system, in which input signals are eventually converted into input variables to the software and

the output control signals are feedback to the controlled environment as a result of the software computation. Although this chapter is dedicated to the documentation and discussion of the hardware related environmental assumptions, a clear delineation of the SOF component (see Figure 5.10), that differentiates it from the rest of the hardware system is necessary and becomes much appreciated when needs arise for investigations of the interface variables.

Relevance: Independent missing assumption.

Likelihood of Change: Likely.

7.4 Environmental Assumptions Concerning the Sensing Circuit: the Band-Pass Filter, the Threshold Detector, and the Amplifier

The following assumptions are made about the sensing circuit of the PACEMAKER's pulse generator.

7.4.1 General

1. A signal detected by the electrode is filtered by a band-pass filter. The signal is then selectively amplified by an amount determined by the programmed sensitivity level and the resultant signal is compared with a preset level at the comparator. Signals of either polarity with magnitude greater than the preset

level enable an input signal to be fed to the timing control circuit of System 1. Signals below the preset level are ignored. In this way greater assurance is given to inhibitions occurring only on the detection of cardiac signals.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the general hardware construction and direction of information flow in the sensing circuit. Should the sensing functionality move from hardware-centric towards software-centric in the future, the software in the future should perform the same functions as documented in this assumption.

Relevance: Independent missing assumption.

Likelihood of Change: Likely.

7.4.2 Band-Pass Filter:

1. The filter is designed to pass signal components in the frequency range of 5-100 Hz, with a centre frequency of 30 Hz.
2. In the design of the filter, the normal ranges (i.e. the set of all possible amplitude and slew rate combinations) for the following signals are known:
 - T waves
 - R waves – normal amplitude range: 6 to 15 mV
 - P waves – normal amplitude range: 1.5 to 2.0 mV
 - PVCs

- Myopotentials

Type: Necessary domain knowledge, descriptive.

Significance: In this assumption, not all of the signals have their corresponding amplitude and slew rate specified. It is still assumed that the amplitude and slew rate of each of the above listed signals is known to the system design engineers for the PACEMAKER system. A thorough understanding of the characteristics of each of the signals in the above list is extremely important, as it directly dictates the design parameters chosen for the bandpass filter. In other words, this assumption is the backbone of the preceding assumption, forming the design rationale for the filter choice specified in the previous assumption (7.4.2.1).

Each signal is characterized by its amplitude and its slew rate. According to their characteristics, these signals can be visualized in a diagram similar to Figure 7.14

Relevance: Independent missing assumption.

Likelihood of Change: Likely.

7.4.3 Amplifier and Threshold Detector

1. The amplifier and threshold detector are designed to operate with detection sensitivity of 1-2 mV.

Type: PACEMAKER hardware design assumption, descriptive.

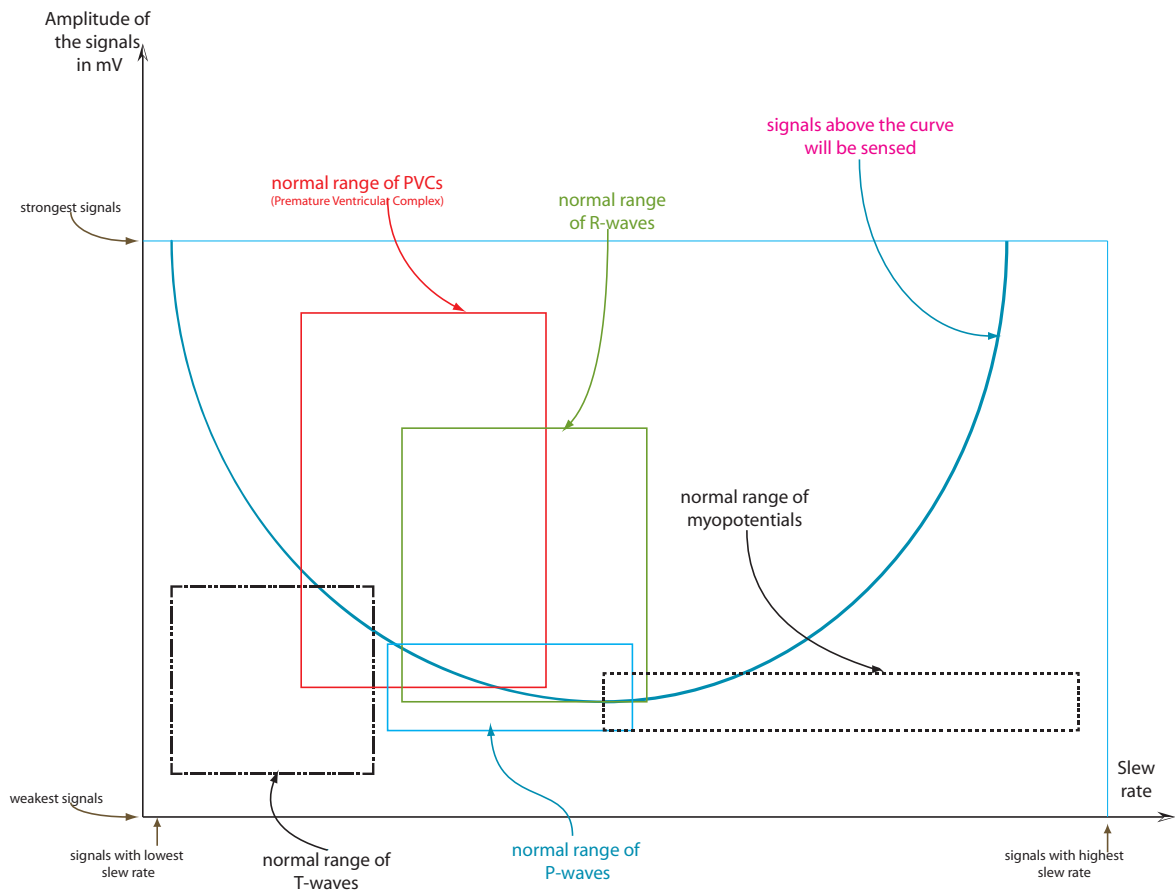


Figure 7.14: The filtering of sensed signals.

Significance: Sensitivity of this order ensures reliable detection of cardiac signals sensed on the electrodes. The cardiac signals typically have amplitudes in the 1-30 mV range depending on the electrode surface area and the sensing circuit loading impedance.

Relevance: Independent missing assumption.

Likelihood of Change: Not likely.

7.5 Environmental Assumptions Concerning the Output Circuit

1. The output circuit determines the amplitude and duration of the stimuli.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption specifies the function of the output circuit in the Pulse Generator.

Relevance: Independent missing assumption.

Likelihood of Change: Not likely.

2. Under normal operating conditions, the timing control circuit determines when the output circuit is triggered. Without any detection of the heart's intrinsic signal, the timing control circuit triggers the output circuit, causing the emission, at the programmed rate. The output pulses are of programmed pulse width and amplitude.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the fundamental mechanism used in controlling the output circuit via the timing circuit. In modern systems, where timing control is performed by the software, this assumption specifies the software's responsibility of ensuring correct behaviour of the pacemaker in terms of delivering pulses at the programmed rate.

Relevance: Independent missing assumption.

Likelihood of Change: Likely.

3. The period between each triggered signal is scrutinized by the rate limiter and in the unlikely event of component failure causing a rate increase, the limiter holds the rate of stimulation to less than 180 ppm.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the fault-recovery method employed by the PACEMAKER system's Pulse Generator. In case of software failure or anomalous outputs (e.g., an upper rate that is faster than the preset URL), the PACEMAKER has a way to recover from the faulty signals sent by the software by using the backup rate limiters.

Relevance: Independent missing assumption.

Likelihood of Change: Not likely.

7.6 Environmental Assumptions Concerning the Timer/Timing Control Circuit

1. The timer defines the time interval between stimuli according to a preset value.

Type: Definitive.

Significance: This seemingly trivial assumption documents an important, fundamental principle in asynchronous pacing. Without any intervention, the simplest form of pacing – asynchronous pacing – would be primarily determined by the inter-stimuli interval set by the timer. In other words, the timer circuit is all there is in terms of simulating the intrinsic heartbeats and controlling the environment during asynchronous pacing.

Relevance: Independent missing assumption.

Likelihood of Change: Not likely.

2. Upon receipt of inhibit signals from System 2, the timing control circuit compares their time of arrival against the programmed refractory period. Signals arriving within the refractory period are ignored. Signals arriving outside the programmed refractory period when zero hysteresis is programmed reset the timer, thus inhibiting the output circuit.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption further explains the response of the output system upon receiving an inhibit signal from System 2. It describes a series

of inter-circuitry interactions, accounting for the presence of a refractory period and zero hysteresis.

Relevance: Independent missing assumption.

Likelihood of Change: Not likely.

3. When hysteresis is programmed, the arrival of a signal outside the refractory period resets the timer, and the escape interval is now the programmed basic interval plus the programmed hysteresis period. Should an inhibit signal be received from System 2 during the period, the timing control circuit resets to again offer the increased escape interval.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption explains the response of the output system upon receiving a sensed signal from System 2. It describes the system's behaviour in terms of a series of inter-circuitry interactions, accounting for the presence of a refractory period and a programmed hysteresis. In hysteresis the electronic escape interval (i.e. the interval between a VS and a VP that immediately follows) is longer than the automatic interval (i.e. the interval between two consecutive VPs). Its purpose is to maintain sinus rhythm and AV synchrony for as long as possible at a spontaneous rate lower (e.g. 50 p.p.m) than the automatic rate of the pacemaker (e.g. 70 p.p.m). Thus when the spontaneous rate drops below 50 p.p.m (in this example), the pacemaker will take over at 70 p.p.m. It will continue to pace at 70 p.p.m, until the spontaneous rate exceeds the automatic

rate, i.e. when the spontaneous QRS complex occurs within the 857 ms automatic interval.

Relevance: To the *PACEMAKER System Specification* – Section 5.8 Hysteresis Pacing.

Likelihood of Change: Not likely.

7.7 Environmental Assumptions Concerning the Battery

1. A lithium-iodine battery is the only pacemaker power source presently used in pacemakers.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption specifies the type of battery that is used in the PACEMAKER system. The long-life lithium-iodine battery powered pacemaker represents a significant advance in pacemaker technology. The lithium battery is solid-state and consists of an anode of metallic lithium (Li) and a cathode of molecular iodine (I_2) bonded in complex form to an organic carrier. Lithium has the highest electrochemical equivalent of any alkali metal. It is, therefore, the most energetic anode material and is ideal for use in high energy density batteries. An anode current collecting screen is pressed between two layers of lithium, forming the anode assembly. The battery develops a voltage of 2.8V (volts), which is

stepped up to 5.4V in the circuitry. No gas is evolved from the simple cell reaction; therefore, the lithium cell can be hermetically sealed in a welded stainless steel enclosure.

Relevance: (a) To *the PACEMAKER System Specification* – Section 4.4 Battery Status.

Likelihood of Change: Not likely.

2. The current drain from the battery (expressed in microamperes, μA) is used to produce the stimulus and to feed the various sensing, detection and house-keeping electronic circuits.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption lays out the units of measurement for the battery's current drain, as well as the various functions powered by the battery within the system.

Relevance: (a) To *the PACEMAKER System Specification* – Section 4.4 Battery Status.

Likelihood of Change: Not likely.

3. Battery capacity expressed in ampere-hours is the quantity that expresses the life time of a lithium-iodine battery.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption specifies the units that are used to express the life time of the battery.

Relevance: (a) To *the PACEMAKER System Specification* – Section 4.4
Battery Status.

Likelihood of Change: Not likely.

4. The output voltage of a fresh cell is 2.8 V (volts), which is then doubled electronically (i.e. 5.4 V) to achieve an output pulse that is close to the amplitude of the human intrinsic cardiac signal (which is approximately 5V).

Type: PACEMAKER hardware design assumption, quantitative.

Significance: This assumption documents the specific output voltage of the PACEMAKER, and gives an explanation of the specific numerical values for the pulse amplitude.

Relevance: (a) To *the PACEMAKER System Specification* – Section 3.4
Pacing Pulse.

Likelihood of Change: Not likely.

5. The lithium-iodine battery shows a continuous, but gradual drop in voltage over a period of years, due to a slow increase in the internal resistance. Once the output voltage has fallen to 3.3V, producing a 6 bpm decline in pulse rate, replacement of the pulse generator is indicated. This happens when internal resistance becomes 35 to 40 k Ω .

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the pivotal issue concerning the battery in the PACEMAKER system – its life time. It suggests a replacement time in terms of the output voltage.

Relevance: (a) To *the PACEMAKER System Specification* – Section 4.4 Battery Status.

Likelihood of Change: Not likely.

6. The cell voltage at the elective replacement point is 2.2-2.4 V.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption also addresses the issue of the battery life time in the PACEMAKER system. It suggests a replacement time in terms of the cell voltage.

Relevance: (a) To *the PACEMAKER System Specification* – Section 4.4 Battery Status.

Likelihood of Change: Not likely.

7. The battery retains a satisfactory voltage for 90% of its life.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the expected length of time during which the system's battery is supposed to function properly.

Relevance: (a) To *the PACEMAKER System Specification* – Section 4.4 Battery Status.

Likelihood of Change: Not likely.

8. The pacemaker replacement time can be determined by measuring the pacemaker rate upon application of a magnet or the battery voltage and/or impedance by telemetry with the Monitor Control Device.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the method and procedure used in replacing the battery.

Relevance: (a) To *the PACEMAKER System Specification* – Section 4.4 Battery Status.

Likelihood of Change: Not likely.

9. A modern pacemaker lasts 7-10 years. When the battery is depleted, the entire pacemaker (excluding the leads) is replaced.

Type: PACEMAKER hardware design assumption, descriptive.

Significance: This assumption documents the estimated life time of the battery. Battery life of internal pulse generators will vary depending on rate and current output settings. At typical rate and output setting of 70 p.p.m and 10 mA respectively, the battery life should be around 7-10 years.

Relevance: (a) To *the PACEMAKER System Specification* – Section 4.4 Battery Status.

Likelihood of Change: Not likely.

Chapter 8

Assumptions Concerning (Software) System Behaviour

Chapter 4 has provided a picture of a general, modern day pacemaker, whose desired behaviour is defined in terms of Timing Cycles. In this chapter, these behavioural requirements on a generic pacemaker are discussed from a software perspective, and are made specific to the PACEMAKER system; assumptions associated with the system's behaviour definition are documented in this chapter.

The documentation of such behavioural assumptions is necessary for the following reasons:

1. It helps the audience of the original PACEMAKER System Specification to understand its content, thus overcoming the threshold posed by hidden assumptions and lack of domain knowledge.
2. It documents part of the rationale behind the design decisions made for the

PACEMAKER system. For example, the reason for including a Blanking Period, or a Refractory Period in the pacemaker's pacing function.

3. It is critical for future development and enhancement of the system. As technology evolves, it is likely that some of the current features the PACEMAKER boasts today will become obsolete and be replaced by newer technology – e.g. more timing cycles may be added to increase the PACEMAKER's level of sophistication in treating certain bradycardiac conditions. In such cases, it is extremely valuable to have a reference to a library of assumptions made on the behaviour of the current PACEMAKER system.
4. It is good practice when it comes to system maintenance.

Like the specification of the pacemaker's system behaviour, the assumptions on the PACEMAKER system behaviour are documented in terms of Timing Cycles. However, assumptions documented in this chapter are 'software-oriented'. In other words, assumptions in this chapter share the common objective of capturing the software implications in the respective areas outlined in the specification, concerning the system's behaviour.

8.1 Another Extension to the Proposed Documentation Convention

The proposed documentation convention for environmental assumptions is further extended in this chapter to accommodate the need for documenting new types of assumptions. The new types of environmental assumptions arise during the investigation of a new class of assumptions, namely those concerning the system's behaviour.

The base types of environmental assumptions – identified in Chapter 6 – are expanded to include the following types:

(Software) system behaviour assumption, descriptive: this type of environmental assumption documents the desired behaviour the (software) system is expected to act in accordance with. It usually exists in the form of a set of 'rules', which collectively defines the set of actions and responses the system can take under specific environmental conditions. This type of assumption also documents the rationale behind the prescribed behaviour of the (software) system, linking the system characteristics back to the properties of its domain environment. Examples from this category include assumptions on the PACEMAKER's responses to sensed signals during various timing cycles, and the influence of events in one chamber of the PACEMAKER upon the other.

(Software) system behaviour assumption, quantitative: this type of environmental assumptions encapsulates important numerical values in determining the desired behaviour of the PACEMAKER system. Examples from this category include the conventionally accepted durations of various timing cycles.

8.2 Timing Cycles In The Eyes Of The Software

An analogy can be used to describe the role performed by the set of rules that defines the behaviour of a medical instrumentation system such as the PACEMAKER system. In the design of software applications dealing with commercial transactions or other operations in the business world, a set of *business rules* are usually abstracted out and modeled as a well-encapsulated component that is separate from the rest of the software system components. This particular abstraction and isolation of system behavioural rules, performed at the design-level, maps well to the PACEMAKER system. In the case of the PACEMAKER system, the set of business rules is replaced by a similar set of ‘rules’ defining the functional behaviour of the system’s software in terms of producing a proper response to the system’s inputs in a timely manner to control its environment.

Timing cycles, viewed in this software-centric context, form the vocabulary which is used to spell out the set of behavioural rules the PACEMAKER system must act in accordance with.

8.2.1 Lower Rate Limit/Interval (LRI)

1. The LRI is the longest interval between a paced or sensed ventricular event and the succeeding ventricular paced event without intervening sensed events.

Type: Definitive

Significance: This assumption defines the timing cycle LRI.

Relevance: To the *PACEMAKER System Specification* – Section 5.1 Lower Rate Limit (LRL)

2. The LRI of the PACEMAKER is ventricular-based in that it is initiated by a paced or sensed *ventricular* event.

Type: (Software) system behaviour assumption, descriptive.

Significance: This clause documents an important assumption: that the PACEMAKER system, and all discussion and specifications followed, is assumed to have ventricular-based lower rate timing. Traditional DDD pacemakers are designed with ventricular-based lower rate timing. In this system a ventricular paced (VP) or ventricular sensed (VS) event initiates the lower rate interval (LRI) and the Atrial Escape Interval (AEI). The AEI always remains constant. In contrary, in the more complex atrial-based lower rate timing, the LRI is initiated and therefore controlled by atrial sensed or paced (AS or AP) events rather than ventricular events.

Relevance: To the *PACEMAKER System Specification* – Section 5.1 Lower Rate Limit (LRL)

8.2.2 Pacemaker Ventricular Refractory Period (VRP)

The pacemaker *Ventricular Refractory Period* is traditionally defined as the period during which the pacemaker is insensitive to incoming signals. However, many pacemakers can now actually sense within part of the refractory period to perform

pacemaker functions (and influence certain timing cycles) other than resetting the Lower Rate Interval (LRI).

1. The PACEMAKER VRP focuses only on the Lower Rate Interval, which cannot be reset or reinitiated by a ventricular signal falling within the refractory interval.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents the fact that the VRP is directly applied to the LRI. The VRP affects the LRI in a way such that it defines a period of time at the beginning of the LRI, where no restarting of the LRI timer is allowed. The manifestation of this constraint on the LRI posed by the VRP is a period of ‘inactiveness’ of the ventricular channel at the beginning of the LRI.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

2. The VRP starts with either a sensed or paced ventricular event; in both cases, the VRPs are equal in duration.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents how the starting point of a VRP is defined. A VRP starts with a ventricular event (either VS or VP), which means it shares the same starting point as the LRI, and overlaps with the first part of the LRI. Furthermore, this assumption also specifies

that the VRPs in both cases are essentially the same, whether initiated by a VS or a VP.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

3. The duration of the pacemaker Ventricular Refractory Period is usually 200-300 ms.

Type: (Software) system behaviour assumption, quantitative.

Significance: This assumption documents the conventionally accepted duration for the VRP, which is adopted in most modern pacemakers. This specification on the duration of the VRP also gives an indication of how much of the LRI should be overlapped by the VRP, i.e., the period of time during which the ventricular channel appears to be inactive.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

4. Pacemaker VRP avoids the sensing of:
 - its own stimulus
 - the paced QRS complex
 - the T wave
 - (excessive) afterpotential
 - the combination of T wave and afterpotential

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption further explains the reason why it is important to have the VRP as one of the most fundamental timing cycles in building the PACEMAKER. It does so by providing a list of undesirable interferences and noise signals whose negative effects are eliminated because of the presence of the VRP.

Relevance: *To the PACEMAKER System Specification* – Section 5.4 Refractory Periods.

5. A ventricular signal generated during the pacemaker ventricular refractory period can never restart another Lower Rate Interval (LRI).

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents one of the ‘rules’ the PACEMAKER software has to act in accordance with. This rule is particularly concerned with the VRP, and it specifies the behaviour of the system during this period. Specifically, the software system is not allowed to start a new LRI upon the detection of a ventricular event during the VRP.

Relevance: *To the PACEMAKER System Specification* – Section 5.4 Refractory Periods.

8.2.3 Atrioventricular Interval (AVI)

1. The AVI is the electronic analog of the PR interval and is designed to maintain AV synchrony between the atria and the ventricles.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents the purpose and importance of the AVI in maintaining the proper functioning of the heart's conduction system.

Relevance: To the *PACEMAKER System Specification* – Section 5.3 Atrial-Ventricular (AV) Delay.

2. AVI is the interval between an atrial event (either sensed or paced) and the scheduled delivery of a ventricular stimulus. In other words, the AVI starts from the atrial stimulus and extends to the following ventricular stimulus or it starts from the point when the P wave is sensed and also terminates with the release of the ventricular stimulus.

Type: Definitive.

Significance: This assumption defines the AVI in terms of its starting and ending points. Effectively, the AVI is the guaranteed, longest period of time possible between an atrial event and a ventricular event that follows immediately after. This is achieved by the PACEMAKER forcing a ventricular pace when the heart fails to track the atrial event on its own at the end of the AVI.

Relevance: To the *PACEMAKER System Specification* – Section 5.3 Atrial-Ventricular (AV) Delay.

3. “Atrial Tracking” is a term used to describe the response of a dual chamber

pacemaker to a sensed atrial event which leads to the emission of a ventricular output pulse.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption explains the concept of “Atrial Tracking”.

Upon sensing a P wave, the PACEMAKER, when in DDD mode, is supposed to ‘track’ the detected atrial activity by providing a corresponding ventricular pace at the expiry of the pre-set AVI.

Relevance: To the *PACEMAKER System Specification* – Section 5.3 Atrial-Ventricular (AV) Delay.

4. The AV intervals may be programmed to fixed values or rate-adaptive (dynamic) i.e. shortening with increasing atrial rates. The rate-adaptive AV interval mimics the physiologic response of the heart:

Relatively slow atrial rate \longrightarrow Longer AVI
Faster atrial rate \longrightarrow Shorter AVI

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents the options available in programming the AVI – it can be modeled as either a constant in the ‘*fixed values*’ mode, or as a variable in the ‘*rate-adaptive*’ mode. The rate-adaptive mode is more advanced in that it mimics the actual physiological response of the heart more accurately. This assumption also outlines the relation between atrial rate and the length of the AVI, thereby specifying the determining factor of the AVI duration in the rate-adaptive mode.

Relevance: To the *PACEMAKER System Specification* – Section 5.3 Atrial-Ventricular (AV) Delay.

5. In healthy individuals at rest, the optimal basic PR or AV interval normally lies between 120 and 210 ms.

Type: (Software) system behaviour assumption, quantitative.

Significance: This assumption documents the normal range of PR interval occurring in healthy hearts. This data provides a base reference for determining the length of the programmable AVI that is to be used as a parameter in the PACEMAKER software system.

Relevance: To the *PACEMAKER System Specification* – Section 5.3 Atrial-Ventricular (AV) Delay.

8.2.4 Atrial Refractory Period

1. It is axiomatic that the atrial channel of a DDD pacemaker must be refractory during the AVI to prevent initiation of a new AVI before completion of an AVI already in progress.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption states one of the ‘rules’ that the PACEMAKER software must act in accordance with in order to be considered as *correct*. This particular rule, concerning the AVI, specifies that the

atrial channel must be blocked during the AVI, i.e., any atrial activity within the AVI should be ignored by the PACEMAKER.

Relevance: To the *PACEMAKER System Specification* – Section 5 Brady-cardia Therapy.

8.2.5 Postventricular Atrial Refractory Period (PVARP)

1. The PVARP begins immediately after the occurrence of a ventricular event – a ventricular pace or a sensed ventricular signal.

Type: Definitive.

Significance: This assumption defines the onset of the PVARP, indicating its association with the occurrence of a ventricular event. The purpose of the PVARP is to prevent the atrial channel from picking up residual signals from the ventricular channel after a ventricular event has occurred. Therefore, the PVARP overlaps with the first part of the LRI, sharing the same starting point.

Relevance: To the *PACEMAKER System Specification* – Section 5.4.3 Postven-tricular Atrial Refractory Period (PVARP).

2. An atrial signal falling within the PVARP cannot initiate a programmed AV interval.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents another one of the ‘behavioural rules’ that the PACEMAKER software must act in accordance with in order to ensure system *correctness*. This particular rule, concerning the PVARP, specifies that the atrial channel must be blocked during the PVARP, i.e., any atrial activity within the PVARP should be ignored by the PACEMAKER.

Relevance: To the *PACEMAKER System Specification* – Section 5.4.3 Postventricular Atrial Refractory Period (PVARP).

3. The PVARP is designed to prevent the atrial channel from sensing the ventricular stimulus, the far-field QRS complex (a voltage that can be seen by the atrial channel), very premature atrial ectopic beats and retrograde P waves.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption further explains the purpose of the PVARP and its significance in preventing cross-talk, noise, and other undesirable interferences in atrial sensing. This assumption documents the list of various types of undesirable signals that are blocked from being sensed by the atrial channel because of PVARP.

Relevance: To the *PACEMAKER System Specification* – Section 5.4.3 Postventricular Atrial Refractory Period (PVARP).

4. The PVARP should be set to a duration longer than the retrograde VA conduction time to prevent the atrial channel from sensing retrograde P waves.

Type: (Software) system behaviour assumption, descriptive.

Significance: In the normal heart, an isolated ventricular event may occasionally be followed by a retrograde P wave because of retrograde ventriculoatrial (VA) conduction (the AV junction being a two-way street). Although this is a physiological phenomenon, it may be hemodynamically unfavourable if it becomes sustained. This assumption documents the actions the system is supposed to take under such situations.

Relevance: To the *PACEMAKER System Specification* – Section 5.4.3 Post Ventricular Atrial Refractory Period (PVARP)

8.2.6 Blanking Periods

General

1. All refractory periods begin with a blanking period. The first part of any refractory period consists of a blanking period during which the pacemaker must not sense at all.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents another one of the “behavioural rules” that the PACEMAKER software must act in accordance with in order to ensure system *correctness*. This particular rule, concerned with the blanking periods in general, specifies the arrangement made between the refractory periods and their associated blanking periods. As a general rule, this assumption dictates that any refractory period must start with

a blanking period. In addition, during the blanking period, the respective channel must be blocked from sensing any incoming signals.

Relevance: To the *PACEMAKER System Specification* – Section 5 Brady-cardia Therapy.

2. The second part of the refractory period permits sensing and each detected event is often represented symbolically by a “refractory sense marker.”

Type: (Software) system behaviour assumption, descriptive.

Significance: As a sequel to the preceding assumption (8.2.6.1), this assumption documents the rule that governs the behaviour of the PACEMAKER software during the second part of the refractory period, i.e., the ‘post-blanking’ refractory period. After the initial blanking period expires, the sensors in the corresponding channel(s) are switched back on during the second part of the refractory period. This allows the sensing of any intrinsic signals. However, signals sensed within this ‘post-blanking’ refractory period are distinguished from the normal VS or AS by designating a special symbolic marker to them. In the PACEMAKER system, these sensed events are marked by bracketed markers. For example, a sensed ventricular event occurring within this ‘post-blanking’ refractory period is denoted as (VS).

Relevance: To the *PACEMAKER System Specification* – Section 5 Brady-cardia Therapy.

Atrial Blanking Period (AB)

1. The atrial channel is completely blocked from sensing any incoming signals during the Atrial Blanking Period, AB.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption specifies the behavioural rule the PACEMAKER is required to follow during an Atrial Blanking Period. This is the ‘atrial-variation’ on the generic rule describing the desired PACEMAKER behaviour during blanking periods from the previous section.

Relevance: To *the PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

2. During the unblanked atrial refractory period, ARP-U, a sensed atrial event cannot initiate an AVI, and is marked using the designation (**AS**).

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption specifies the exact behaviour the PACEMAKER software is required to implement during the unblanked atrial refractory period.

Relevance: To *the PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

3. The atrial channel is completely blocked from sensing any incoming signals during the Atrial Blanking Period, AB.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption is a behavioural rule that specifies the proper reaction of the PACEMAKER towards incoming signals in the atrial channel during the AB.

Relevance: To *the PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

Ventricular Blanking Period (VB)

1. The detection of all signals in the ventricular channel is blocked during the Ventricular Blanking Period, VB.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption is a behavioural rule that specifies the proper reaction of the PACEMAKER towards incoming signals in the ventricular channel during the VB.

Relevance: To *the PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

2. During the unblanked ventricular refractory period, VRP-U, signals can be detected but neither the Atrial Escape Interval nor the Lower Rate Interval can be reinitiated. A ventricular event sensed during VRP-U is marked using the designation (**VS**).

Type: (Software) system behaviour assumption, descriptive.

Significance: The detected signals in the VRP-U can be used by the pacemaker to control some timing cycles for a variety of functions while the LRI remains unaffected.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

3. Blanking periods can be free-standing and need not necessarily be followed by an unblanked refractory period such as VRP-U.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption clarifies the relation between a blanking period and a VRP-U, which may or may not come immediately after the blanking period.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

Postatrial Ventricular Blanking (PAVB) Period

If the atrial stimulus interferes with the ventricular channel, the disturbance is called *crosstalk*. The atrial stimulus, if sensed by the ventricular channel, can cause ventricular inhibition.

1. Prevention of crosstalk is mandatory and requires the addition of a brief ventricular blanking period beginning coincidentally with the release of the atrial stimulus. This is known as the Postatrial Ventricular Blanking (PAVB) Period

– a brief ventricular interval initiated by an atrial pace when the ventricular sensing amplifier is switched off.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents the addition of an important blanking interval, which results in a DDD pacemaker having five basic timing cycles and two derived timing cycles. This format was the basis of first generation DDD pacemakers that were clinically used and accepted. Even a sophisticated contemporary DDD pacemaker reduced to having only these seven intervals would function satisfactorily if appropriately programmed. Further addition of timing cycles represents refinements rather than essential elements of DDD pacing.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

2. The ventricular channel is switched off during the Postatrial Ventricular Blanking (PAVB) period. No signal can be detected in the ventricular channel during the PAVB period. The ventricular channel then opens after this short blanking period so that ventricular sensing (with reset of the Atrial Escape Interval and the LRI) can occur during the remainder of the AVI.

Type: (Software) system behaviour assumption, descriptive.

Significance: The PAVB is introduced to offset the unfavourable influence an atrial paced signal could have on the ventricular channel. The sequence

of behavioural rules that ensures the prevention of cross-talk is specified in this assumption.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

3. PAVB prevents AV crosstalk or sensing of the atrial stimulus by the ventricular channel.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents the purpose and the end result of incorporating the PAVB as one of the essential timing cycles.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

4. PAVB is usually programmed to be a brief interval - 10 to 60 ms - initiated by an atrial paced event.

Type: (Software) system behaviour assumption, quantitative.

Significance: This assumption provides the normally expected range of durations for a PAVB. No PAVB after atrial sensing is initiated. PAVB is only applicable for paced atrial events.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

8.2.7 Upper Rate Interval (URI)

1. URI is the speed limit to control the response of the ventricular channel to sensed atrial activity. To define URI formally: the URI of any DDD pacemaker is the interval between two consecutive ventricular stimuli or between a sensed ventricular event and the succeeding ventricular stimulus while maintaining 1:1 AV synchrony with sensed atrial events.

Type: Definitive

Significance: This assumption defines the timing cycle URI. For example, if the URI is 500 ms (upper rate = 120 p.p.m.), a P wave occurring earlier than 500 ms from the previous atrial event (atrial rate faster than 120 p.p.m.) will not be followed by a ventricular stimulus. Such an arrangement allows atrial sensing with 1:1 AV synchrony between the lower rate and the upper rate.

Relevance: To the *PACEMAKER System Specification* – Section 5.2 Upper Rate Limit (URL).

2. A P wave occurring earlier than the programmed URI will not be followed by a ventricular stimulus. Such an arrangement allows atrial sensing with 1:1 AV synchrony between the lower rate and the upper rate.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents the behavioural rule the PACE-MAKER has to follow in order to achieve 1:1 AV synchrony. In other

words, the PACEMAKER is required to track only those intrinsic atrial events occurring at a rate lower than the URL. Any sensed P wave that results in a rate faster than the preset URL is ignored by the PACEMAKER.

Relevance: To the *PACEMAKER System Specification* – Section 5.2 Upper Rate Limit (URL).

3. A URI programmable independently of the Total Atrial Refractory Period (TARP) provides a smoother upper rate response than the rather abrupt slowing when the TARP is the only interval controlling the upper rate.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents the purpose and advantages of the presence of a programmable URI, as opposed to using solely the TARP as an upper bound to control the output rate of the PACEMAKER.

Relevance: To the *PACEMAKER System Specification* – Section 5.2 Upper Rate Limit (URL).

8.2.8 Ventricular Safety Pacing Window (VSP)

The Ventricular Safety Pacing Window complements the PAVB in dealing with crosstalk – this function does not prevent crosstalk but merely offsets its consequences.

1. By convention the VSP starts at the time of an atrial paced event, AP, and its duration is usually 100 to 110 ms.

Type: (Software) system behaviour assumption, quantitative.

Significance: This assumption documents the starting point and the duration of the VSP. By convention, the length of the VSP is usually 100 to 110 ms. The reason behind this specific duration is that the intrinsic P-R intervals are usually longer than 100 to 110 ms, therefore the VSP is the minimum period of time which will enforce the proper functioning of the heart. It is also for this reason that the VSP window is often called a *non-physiological AVI*.

Relevance: To *the PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

2. The PAVB period, also activated by the atrial stimulus, occupies the initial portion of the VSP.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption stresses the relation between the PAVB and the VSP - both are introduced to handle situations where crosstalk might be a problem. The PAVB is significantly shorter than the VSP, and it overlaps with the first part of the VSP, during which no sensing in the ventricular channel is enabled. After the programmed PAVB times out, the ventricular channel is turned back on, and any intrinsic signal sensed during this particular portion of the VSP is remembered by the PACEMAKER and is used to make decisions on the PACEMAKER's corresponding response.

Relevance: To *the PACEMAKER System Specification* – Section 5 Brady-cardia Therapy.

3. Ventricular sensing cannot occur during the VSP.

Type: (Software) system behaviour assumption, descriptive.

Significance: Ventricular sensing can occur in the VSP only after completion of the relatively short PAVB period.

Relevance: To *the PACEMAKER System Specification* – Section 5 Brady-cardia Therapy.

4. The three cases encountered in ventricular safety pacing and the corresponding response of the PACEMAKER are:

(a) No spontaneous conduction, no crosstalk, no interference: ventricular pace, VP, at the end of the programmed AVI.

(b) Interference (or premature ventricular events) during the VSP window (beyond the PAVB) results in a committed ventricular pace, VP, at the end of the VSP window and a characteristic shortening of the AVI.

(c) A sensed ventricular event, VS, occurs after the VSP but before the AVI times out: normal inhibition of the ventricular channel will occur.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption describes the three important scenarios to consider in understanding the VSP. The corresponding PACEMAKER

response in each of the three scenarios further confirms the fact that VSP is introduced to help alleviate the negative effect of crosstalk. Essentially, VSP offsets the consequences of crosstalk by forcing a paced ventricular event for any ventricular activities sensed within the VSP window. At the same time, VSP fulfills the physiological requirement of maintaining a proper AV delay of at least the minimal length, i.e., 100 to 110 ms.

Relevance: To the *PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

Derived Timing Cycles

The four basic timing cycles of a simple DDD pacemaker consist of: LRI, VRP, AVI, and URI. Additional timing intervals can be derived from these four basic intervals.

8.2.9 Atrial Escape Interval (AEI)

1. The AEI is defined as:

$$\text{AEI} = \text{LRI} - \text{AVI}$$

Type: Definitive

Significance: This assumption defines the timing cycle AEI in terms of the LRI and the AVI. The AEI is crucial in the analysis of DDD pacemaker function because it represents the interval the pacemaker uses to determine when the next atrial stimulus should occur after a sensed or paced ventricular event.

Relevance: To *the PACEMAKER System Specification* – Section 5 Brady-cardia Therapy.

2. In DDD pacemakers with ventricular-based lower rate timing, the atrial escape interval always remains constant after programming the lower rate interval and AV delay.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption is derived from the previous one. It further lays out the relations between AEI, AVI, and LRI, and how they are interrelated.

Relevance: To *the PACEMAKER System Specification* – Section 5 Brady-cardia Therapy.

8.2.10 Total Atrial Refractory Period (TARP)

1. The TARP is defined as:

$$\text{TARP} = \text{AVI} + \text{PVARP}$$

Type: Definitive

Significance: This assumption defines the timing cycle TARP. It also documents the relation TARP has with AVI and PVARP.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

2. The duration of the TARP always defines the shortest *upper rate* or the fastest paced ventricular rate.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption documents the importance of the TARP in defining the behaviour of the PACEMAKER system. The AVI, PVARP and the upper rate interval are interrelated in a simple DDD pacemaker without a separately programmable upper rate interval. In such a system, the upper rate interval is controlled solely by the duration of the TARP according to the formula: Upper Rate (p.p.m.) = 60000 / TARP (ms).

When the interval between consecutive P waves becomes shorter than the TARP, tracking of every P wave becomes impossible. Every alternate P wave will fall in the PVARP where it cannot initiate an AVI. The pacemaker will thus respond to the P waves in a 2:1 fashion. This form of upper rate response is called 2:1 block and the TARP effectively becomes the URI.

Relevance: To the *PACEMAKER System Specification* – Section 5.4 Refractory Periods.

8.3 Influence of Events in One Chamber upon the Other

The operation of the two channels of a DDD pacemaker are intimately linked – an event detected by one channel generally influences the function of the other.

8.3.1 Atrial Channel

In a normal heart, an atrial event must always be followed by a ventricular event after some delay. A sensed atrial event alters pacemaker function in two ways:

1. It *triggers* a ventricular stimulus (after a delay equal to the AV interval) provided the ventricular channel senses no signal during the AV interval.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption describes the notion of “atrial tracking” where the AV synchrony of a normal heart is maintained by requiring the pacemaker to schedule a ventricular paced event after the sensing of an intrinsic atrial event.

Relevance: To *the PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

2. It *inhibits* the release of the atrial stimulus that would have occurred at the completion of the atrial escape interval. In other words, it aborts the AEI before it can time out.

Type: (Software) system behaviour assumption, descriptive.

Significance: While the previous assumption describes the desired PACEMAKER behaviour in the ‘triggered’, T, mode, this assumption documents the required response of the PACEMAKER functioning in the ‘inhibited’, or I, mode. A sensed, intrinsic atrial event will automatically inhibit the firing of an atrial pace by the PACEMAKER, and reset the PACEMAKER’s internal timer for the AEI. Therefore, the atrial channel functions simultaneously in the triggered mode – to deliver the ventricular stimulus for AV synchrony – and in the inhibited mode to prevent competitive release of an atrial stimulus after sensing a P wave. In contrast to the atrial channel, the ventricular channel functions only in the inhibited mode.

Relevance: To the *PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

8.3.2 Ventricular Channel

1. A sensed ventricular event *outside the AVI* such as a ventricular extrasystole (or Premature Ventricular Complex, PVC) will inhibit the atrial and ventricular channels. The AEI in progress is immediately terminated and release of the atrial stimulus inhibited. The sensed ventricular event also inhibits the ventricular channel and initiates a new atrial escape interval. Thus both the atrial and ventricular channels are inhibited simultaneously.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption outlines the effects of an abnormal ventricular sense (i.e., a PVC) on both the ventricular channel and the atrial channel. In terms of the ventricular channel, the manifestation of sensing a PVC is that the Lower Rate Interval, LRI, gets reset immediately, thereby inhibiting the delivery of a ventricular pace at the end of the original LRI. In a similar manner, the atrial channel is inhibited by the detection of a PVC: the AEI is reset, and an atrial paced event is only released after the new AEI expires.

Relevance: To *the PACEMAKER System Specification* – Section 5 Bradycardia Therapy.

2. When a ventricular event is sensed *within the AVI* there is no need for the pacemaker to release a ventricular stimulus at the completion of the AV delay because spontaneous ventricular activity is already in progress. Therefore the pacemaker aborts the AV delay by virtue of the sensed ventricular event. The AV delay is thus abbreviated. The sensed ventricular event immediately starts a new AEI.

Type: (Software) system behaviour assumption, descriptive.

Significance: This assumption outlines the effects of a normal ventricular sensed event, VS, on the ventricular channel and the atrial channel. In terms of the ventricular channel, the manifestation of a VS is the termination of the previous Lower Rate Interval, LRI, inhibiting the delivery of

an unnecessary ventricular pace. In a similar manner, the atrial channel is inhibited by a VS and two timing cycles are reset: both the AVI and the AEI. As a result, the 'actual' AVI as seen on the ECG appears to have been shortened, and an atrial paced event is only released after the new AEI expires.

Relevance: To the *PACEMAKER System Specification* – Section 5 Brady-cardia Therapy.

Chapter 9

Other Environmental Assumptions Concerning System Boundaries

B1.2 and B1.4

In this thesis, a significant amount of work is put into the identification and documentation of environmental assumptions concerning system boundary **B1.1** – the PACEMAKER’s interface to its encompassing physiological domain – and **B2**, the hardware interface. While the study of environmental assumptions at **B1.1** and **B2** remains the main concentration of this thesis, potential environmental assumptions at **B1.2** (the interface concerning the application of a medical magnet) and **B1.4** (the communication interface between the PACEMAKER’s Pulse Generator and the Device Controller-Monitor) are also of interest. In addition, for the purpose of demonstration, the proposed documentation convention is applied again in this

chapter to document the environmental assumptions found on system boundaries **B1.2** and **B1.4**.

Therefore, this chapter identifies and documents environmental assumptions related to **B1.2** and **B1.4** in the PACEMAKER model, presenting another example of applying the proposed convention for documenting environmental assumptions in general. However, this chapter does not provide a *complete* list of environmental assumptions associated with the system boundary **B1.4**. As discussed earlier in Chapter 6, the magnitude of the problem concerning the serial communication between the PACEMAKER's pulse generator and the Device Controller-Monitor (DCM) is beyond the scope of this thesis. As a result, for **B1.4**, only environmental assumptions that are considered as being directly related to the PACEMAKER project are documented.

9.1 Further Extension to the Proposed Documentation Convention

The proposed documentation convention for environmental assumptions is further extended in this chapter to accommodate the needs for documenting new types of assumptions. The new types of environmental assumptions arise during the investigation of a new class of assumptions, namely those concerning the system boundaries **B1.2** and **B1.4**.

The base types of environmental assumptions – introduced in Chapter 6 – are expanded to include the following types:

Magnet assumption: this type of environmental assumption is related to the PACEMAKER's behaviour upon the application of a medical magnet.

Communication assumption: this type of environmental assumption encapsulates important background information characterizing the serial communication between the Device Controller-Monitor and the PACEMAKER's Pulse Generator.

9.2 Environmental Assumptions Concerning System Boundary B1.2 – the Magnet Interface

In Section 3.7 Magnet Test, the original *PACEMAKER System Specification* states that:

“...A standard cardiac donut magnet shall be detected by the device at a distance of 2.5 cm between the center of the labeled surface of the device and the surface of the magnet...”

Further requirements characterizing the PACEMAKER's behaviour in the Magnet Mode are also specified in the original *PACEMAKER System Specification*, including:

“When the magnet is in place, the device shall:

1. Pace asynchronously with a fixed pacing rate. The device mode shall be AOO if previous mode was AXXX, VOO if previous mode

was VXXX, DOO if previous mode was DXXX, or OOO if previous mode was OXO modes.

2. ...
3. When the magnet is removed the device shall automatically assume pretest operation.
4. The magnet mode shall have the capability to be programmed OFF, so that it will ignore magnet detection.

”

Environmental Assumptions Concerning System Boundary

B1.2

The following environmental assumptions are identified in support of the system requirements specified in the original *PACEMAKER System Specification*.

1. The magnet mode refers to the response of a pacemaker when a magnet is applied over it.

Type: Magnet assumption.

Significance: This assumption specifies the pre-condition that must be satisfied before the PACEMAKER can enter the ‘magnet mode’. In other words, applying a medical magnet on the surface of the patient’s body triggers the initiation of the magnet mode within the PACEMAKER’s Pulse Generator (PG). The original *PACEMAKER System Specification*

further outlines the desired behaviour of the PACEMAKER when it is operating within the magnet mode.

Relevance: To the *PACEMAKER System Specification* – Section 3.7 Magnet Test.

2. The magnet closes the special reed-switch within the Pulse Generator causing the PG to pace at the asynchronous mode at the magnet rate.

Type: Magnet assumption.

Significance: This assumption explains the mechanism used by the PG to detect the presence of a medical magnet, namely via the opening and closing of an embedded reed-switch inside the PG.

Relevance: To the *PACEMAKER System Specification* – Section 3.7 Magnet Test.

3. The behaviour of the magnet mode and the magnet rate vary according to the manufacturer.

Type: Magnet assumption.

Significance: This assumption documents the fact that the behaviour of a specific pacemaker under the magnet mode is vendor-specific. For the PACEMAKER system, the desired magnet-mode-behaviour is specified in Section 3.7 of the original *PACEMAKER System Specification*.

Relevance: To the *PACEMAKER System Specification* – Section 3.7 Magnet Test.

4. The magnet mode is used to assess pacemaker function and battery depletion.

Type: Magnet assumption.

Significance: This assumption documents the main purposes of the magnet mode. In addition, it also explains when the magnet mode should be used.

Relevance: To the *PACEMAKER System Specification* – Section 3.7 Magnet Test.

5. The magnet mode can be programmed “off” in some pacemakers.

Type: Magnet assumption.

Significance: This assumption documents the option for the PACEMAKER to be irresponsive towards the presence of a medical magnet, i.e. the application of a magnet will not trigger the PACEMAKER to switch to asynchronous pacing.

Relevance: To the *PACEMAKER System Specification* – Section 3.7 Magnet Test.

9.3 Environmental Assumptions Concerning System Boundary B1.4 – the Serial Communication Interface

The PACEMAKER system consists of three major components:

- Pulse Generator (PG)
- Device Controller-Monitor (DCM) and associated software
- Leads

Among these, the Device Controller-Monitor (DCM) is the primary implant, pre-discharge Electrophysiology (EP) support, and follow-up device for the PACE-MAKER system. The DCM communicates with the PG using a communication protocol and supporting hardware. The DCM in turn consists of the following:

- A hardware platform
- PACEMAKER application software

The features of the DCM are listed in Section 2.2.2 Device Controller-Monitor (DCM) Overview of the original *PACEMAKER System Specification*.

System requirements specifying the communication characteristics between the DCM and the PG are documented in Section 3.2.6 DCM-PG Telemetry of the original *PACEMAKER System Specification*. It states that:

“The DCM shall either:

- use an inductive telemetry wand to communicate with the pulse generator, maintaining consistent communication over the range of 0 cm to 5 cm between the wand and the pulse generator; or,
- use some other medium, such as RF or ultrasound, that is safe and legal to use, for maintaining consistent telemetry with an implanted medical device.

”

Environmental Assumptions Concerning System Boundary

B1.4

Environmental assumptions associated with the communication sub-environment are identified and documented here in support of the corresponding system requirements specifications.

1. Data transmission between the DCM and the PG is achieved via one of several communication techniques. The commonly used communication methods are:
 - (a) **magnetic** – an electromagnet placed on the surface of the body establishes a magnetic field which penetrates the skin and operates the pacemaker’s reed switch.
 - (b) **radio-frequency waves** – the information can be transmitted over high frequency electromagnetic waves which are received inside the body by an antenna. The antenna is usually in the shape of a coil housed within the PG.
 - (c) **acoustic-ultrasonic pressure waves** – acoustic-ultrasonic pressure waves generated from a suitable transducer placed over the skin, can penetrate the human body. They are received by a suitable receiver in the PG which carries out the desired function.

Type: Communication assumption.

Significance: This assumption documents all the communication methods available to the PACEMAKER system. Out of all these methods, the magnetic field method is the most widely used because of its simplicity and minimal power requirements. A functional block diagram depicting the communication interface involving the use of an electromagnet is presented in Figure 9.15.

Relevance: To the *PACEMAKER System Specification* – Section 3.2.6 DCM-PG Telemetry.

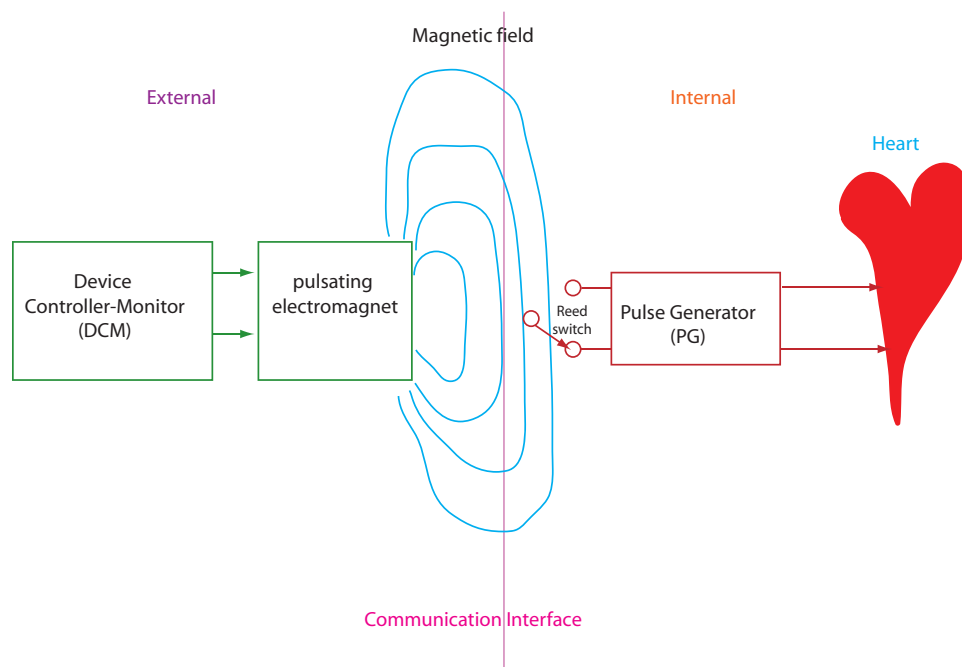


Figure 9.15: Functional block diagram of the magnetic communication interface.

2. In the case where magnetic field is used as the communication medium, the

programming system of the PACEMAKER requires preliminary closure of the reed switch before a command is transmitted from the DCM to the PG.

Type: Communication assumption.

Significance: This assumption documents the pre-condition that must be met before enabling data transmission between the DCM and the PG.

Relevance: *To the PACEMAKER System Specification* – Section 3.2.6 DCM-PG Telemetry.

3. The Pulse Generator is non-invasively programmable, enabling the following parameters (including but not limited to) to be altered: Mode, LRL, URL, Maximum Sensor Rate, pulse width, pulse amplitude, sensitivity, refractory period and hysteresis.

Type: Communication assumption.

Significance: Appendix A of the original *PACEMAKER System Specification* documents the complete set of programmable parameters that are applicable to the PACEMAKER system. The programmable values, increments, nominal values, and tolerances are also specified for each of the programmable parameters in Appendix A.

Relevance: *To the PACEMAKER System Specification* – Section 3.2.6 DCM-PG Telemetry.

4. The DCM contains a microprocessor-based transmitter/receiver that operates by inductively coupling pulse-position modulated, binary coded data from the

DCM via the programming wand to the PG.

Type: Communication assumption.

Significance: This assumption specifies the characteristics of the information-carrying signal emitted by the DCM. The signal implements pulse-position modulation and is encoded as a sequence of bits.

Relevance: To the *PACEMAKER System Specification* – Section 3.2.6 DCM-PG Telemetry.

5. The programming information is contained in a 20-bit command code specifying the desired rate, pulse width, pulse amplitude, sensitivity level, mode of operation, a PG model identification code and check bits.

Type: Communication assumption.

Significance: An essential requirement of programmable pacemakers is that they should be immune to accidental programming from naturally occurring energy sources. To meet this requirement, the information is usually coded and the pacemaker contains a decoding mechanism to recognize proper information. This security code method makes it practically impossible to reprogram an implantable pacemaker through extraneous random magnetic fields.

If an attempt is made intentionally or unintentionally to include in a programming command a parameter that is not a feature of the PG being used, that parameter will simply remain at its nominal value. All valid

reprogrammed parameters in the command will be implemented. Part of the command code is a number of check bits. If these check bits are not correct, the command is rejected by the PG, and no programming occurs.

Relevance: To the *PACEMAKER System Specification* – Section 3.2.6 DCM-PG Telemetry.

6. The timing of the transmission is precise. Crystal oscillators in both the DCM and the PG control the frequency of data exchanges. Each data bit is transmitted within approximately 1.0 ms. The entire command code is transmitted within approximately 40 ms or 1/25th of a second.

Type: Communication assumption.

Significance: This assumption stresses the importance of timing in the DCM-PG communication paradigm. It gives an indication (in seconds/bit) of the speed of data transmission between the DCM and the PG.

Relevance: To the *PACEMAKER System Specification* – Section 3.2.6 DCM-PG Telemetry.

Chapter 10

Lessons Learned from the Identification and Documentation of Environmental Assumptions in the PACEMAKER Project

This thesis documents the research findings revolving around the PACEMAKER project. More specifically, it identifies and documents the environmental assumptions that arise during the system specification process of the PACEMAKER. The environmental assumptions are identified at both the requirement level as well as the design level. The ultimate contribution of this thesis is that it identified steps one can take to include environmental assumptions in documenting requirements for applications such as PACEMAKER. The final outcome is a complete system specification

that provides references to various classes of environmental assumptions associated with the PACEMAKER system.

Valuable lessons were learned during the course of finding these environmental assumptions within the PACEMAKER system. These include the systematic methodology developed during the process of finding the hidden environmental assumptions. The steps and method used are presented as individual chapters throughout the thesis along with their end results, which are the actual assumptions identified.

Also, in this thesis, a convention was proposed for the documentation of the identified environmental assumptions. Evolving from its most primitive form, the initial format of the convention has been extended incrementally at various stages, fully demonstrating the flexibility and extensibility of the proposed documentation system. The elements provided by the documentation system are aimed to capture the full spectrum of characteristics of a single environmental assumption (e.g. its type, significance, relevance, etc.).

In addition, all the lessons learned presented in this chapter are not specific to the PACEMAKER project, nor are they specific to medical instrumentation devices – instead, they provide valuable insights and a good application example for any system involving a software component; they can be easily generalized, extended or modified to suit the needs for identifying and documenting environmental assumptions in other non-medical, software-centric systems.

As a summary and an overall assessment of the PACEMAKER project, this chapter ties together each individual chapter in this thesis. It does so by drawing relations

among the important concepts introduced in these chapters, and making logical connections between the procedural steps that are identified and used throughout the PACEMAKER project. This chapter also reviews the process of identifying and documenting environmental assumptions at an integrated level. It provides an overview and assessment of the adopted procedure, as well as documenting valuable insights that are the ultimate outcomes of this thesis/research. By putting all the pieces together, this chapter renders a grand picture of all the lessons learned during the course of the PACEMAKER research project.

Each lesson presented here is intended to target an audience that is wider than those who are only interested in medical instrumentation systems. The lessons are made generic enough that they can be applied to other embedded computer systems outside of the medical arena.

10.1 Lesson 1: Domain investigation – Identify the search space for environmental assumptions, start with the most generic

One of the major challenges faced by PACEMAKER project was the effective integration of domain knowledge into a formal system specification that is to be read and understood by both domain experts and system engineers. To address this issue, the research presented in this thesis started with a broad-spectrum search of commonalities and property-defining constraints within the domain environment of

the PACEMAKER, namely the world of medical instrumentation systems.

This thesis first defines the PACEMAKER system as a system that extended from the more generic class of artificial cardiac pacemakers, which, when viewed with an even higher level of abstraction, is a subclass of medical instrumentation systems. Through this abstraction, the research described in this thesis was able to delineate the boundary of an initial search space to include all commercial medical instrumentation systems.

Chapter 2 of this thesis explored the first principles involved in a medical instrumentation system. This broad-spectrum investigation revealed a set of general design constraints, performance requirements, and government regulations that are applicable to all commercial medical instrumentation systems. As a lesson learned, it is extremely important to form an initial search space where future environmental assumptions may be elicited. The initial search space should be generic enough to not leave out any potential candidates for future environmental assumptions.

10.2 Lesson 2: Prune the search space by studying the characteristics and constraints present in current mainstream artificial pacemakers

By modeling the medical instrumentation system as a control system and defining its components, more domain specific assumptions were further discovered. A component-wise system architecture for a basic medical instrumentation system was

sketched out in the beginning phase of this research. It was used to outline the common structures involved in a control system. This generic model was later further developed to map to the pacemaker system. Doing so narrowed the search space and pruned the initial large set of assumptions, keeping the search space more domain specific.

General constraints in the design of medical instrumentation systems were elicited. Many factors imposed constraints on the design of general medical instrumentation systems, and were discovered through search space pruning. For example, *Accessibility of the Signal Source*, *Variability of Physiological Parameters*, *Interference among Physiological Systems*, *Sensor Interface Problems*, and *Safe Levels of Applied Energy*. Based on these constraints, additional environmental assumptions were explored in the areas of *Signal Consideration*, *Environmental Considerations*, *Medical Considerations*, and *Economic Considerations* .

10.3 Lesson 3: Study the domain environment extensively and understand the critical requirements posed by the encompassing environment on the control system

By studying the domain environment of the pacemaker, i.e. the anatomy of the heart, important features of the biological environment were revealed. For example, in the in-depth investigation of the heart's electrical conduction system, it was identified

that the delay at the AV node is crucial, as it allows enough time for all of the blood in the atria to fill their respective ventricles. This AV-interval is one of the many programmable timing intervals found in modern day pacemakers. It is also one of the four most fundamental timing intervals that constitute the grounds on which an artificial pacemakers essential functionality is built. Similarly, requirements for effective pumping were derived from studying the electrophysiology of the heart. Owing to the exquisite intricacy of the heart's electrophysiology, a set of critical requirements exists on the cardiac electrical conduction system for the effective functioning of the heart. These include a substantial atrial to ventricular delay, the coordinated contraction of ventricular cells, and the absence of tetany.

The nature and properties of the domain environment dictate the operational characteristics of the control system. Therefore, domain environment research is essential in the search for environmental assumptions in the Pacemaker project. This idea, or lesson learned, can be extrapolated and used in similar projects that deal with boundary analysis between a controlled environment and its controlling system.

10.4 Lesson 4: Thoroughly understand the device or control system under consideration

Immediately following domain investigation, a comprehensive survey of the control system, the artificial pacemaker in this case, was carried out. This in-depth study of the modern pacemaker system allowed the definition and understanding of concepts and terminology that were later used in specifying the environmental assumptions

found at different system boundaries. Examples of such crucial concepts include the programmability of the pacemaker, the basic set of programmable variables and their effects, and the functional behaviour of a (simple) DDD pacemaker, described in terms of nine DDD Timing Cycles.

10.5 Lesson 5: Model the system

One of the most important contributions of this thesis is the method it proposes to model the control system. The model presented was designed specifically to aid the elicitation and documentation of environmental assumptions. It defines system boundaries at different levels of specificity, based on which environmental assumptions of different types and categories were determined and documented.

The PACEMAKER System is identified as an embedded, process-control system, with a specialized medical application. Several precise notations have been developed to specify software requirements for embedded, *reactive systems* – among which, the Software Cost Reduction (SCR) notation [15], Statecharts, and the Requirements State Machine Language (RSML) have received considerable attention. The model proposed in this thesis is a variation of Parnas' Four-Variable Model (FVM) [23], which is used in SCR and the version of Parnas' Rational Design Process used in Ontario Power Generation's Safety-Critical Software Methods.

10.6 Lesson 6: Identify system boundaries and interfaces

The proposed model breaks the domain environment of the PACEMAKER System down into a number of smaller, mutually exclusive sub-environments. Modeling the PACEMAKER system and drawing system boundaries and specifying interfaces at each of these boundaries were greatly driven by the need for properly identifying environmental assumptions for the system. In the PACEMAKER model, two major system boundaries were defined.

The first system boundary (**B1**) was drawn between the complete PACEMAKER system and its domain environment. **B1** consists of four sub-boundaries (**B1.1** – **B1.4**), each specifying:

1. the pacemaker's interaction with its physiological environment, namely the heart (**B1.1**);
2. the pacemaker's response to the application of a medical magnet (**B1.2**);
3. the pacemaker's corresponding behaviour when the use of an accelerometer is enabled (**B1.3**);
4. the serial communication between the pacemaker's pulse generator and its external control unit (**B1.4**).

The second system boundary, **B2**, defines the interface between the system hardware and the system software.

10.7 Lesson 7: Elicit environmental assumptions at each system boundary/interface

In the proposed PACEMAKER system model, the domain environment was divided into four sub-domains – the biological, the communication, the magnet, and the accelerometer sub-domains. These four sub-domains, although sharing the same system boundary, are very different, and so are the environmental assumptions associated with each.

One valuable lesson learned in the PACEMAKER project research is the procedure that was developed to identify and document environmental assumptions at each predefined system boundary. Environmental assumptions were identified, refined, classified, and documented pertaining to a specific system boundary. For example, at system boundary **B1.1**, a set of environmental assumptions for the PACEMAKER system concerning the biological interface was elicited. Also, the identification of a second system boundary (**B2**) allowed the documentation of another type of environmental assumptions, those made on the systems hardware. Furthermore, behavioural requirements on a generic pacemaker are also discussed in this thesis (from a software perspective). As a result, assumptions associated with the systems behaviour are also identified and documented.

While the study of environmental assumptions at **B1.1** and **B2** remains the main concentration of this thesis, potential environmental assumptions at **B1.2** (the interface concerning the application of a medical magnet) and **B1.4** (the communication

interface between the PACEMAKERs Pulse Generator and the Device Controller-Monitor) were also of interest. In addition, for the purpose of demonstration, the proposed documentation convention was also applied to document the environmental assumptions found on system boundaries **B1.2** and **B1.4**.

10.8 Lesson 8: Refine environmental assumptions at each level of specificity

The initial set of environmental assumptions extracted needs further refinement. This primitive, broad set of environmental assumptions may contain information that is either too descriptive, qualitative, or even irrelevant to the original PACEMAKER System Specification.

The refinement process proposed in this thesis starts with looking at each of the elicited assumptions individually and asking the following three questions:

1. What – What kind of assumption is it? The type of assumption defines whether an assumption is *definitive*, *descriptive*, or *quantitative*.
2. Why – Why is it important/necessary to document this assumption? What is its significance in terms of aiding system requirements specification, design documentation, future system upgrades, and maintenance?
3. How – How is it related to the original PACEMAKER System Specification? In what respect does the assumption help to clarify the original requirements document?

By asking these three questions, peripheral assumptions are weeded out leaving only the essential environmental assumptions to document.

10.9 Lesson 9: Classify the environmental assumptions

It is important to identify the type of an environmental assumption, as classification allows better documentation and easier future reference.

The type of environmental assumptions identified for the PACEMAKER system at system boundary **B1.1** fall into the following four general types:

Definitive: this type of assumption is essentially a missing definition on some vague term in the original PACEMAKER System Specification. It helps clarify the meaning of clauses in the original document, enhances its readability, and removes some of the domain knowledge related barrier for the reader of the original PACEMAKER System Specification.

Necessary domain knowledge, descriptive: this type of assumption states domain-knowledge-related necessary conditions for the proper/correct functioning of the PACEMAKER system. Examples from this category include assumptions resulting from the requirements for effective pumping of the heart and assumptions on the cardiac cycle.

Necessary domain knowledge, quantitative: this type of assumption documents necessary, quantitative domain knowledge in a precise manner with specific numerical values. Because of its quantitative nature, this type of environmental assumption is easily verified; these assumptions put constraints directly on the design decisions system engineers have to make. Examples from this category include the assumptions made on the range of the bioelectric signal, assumptions on the normal human heart rate at rest, and the various firing rates of natural pacemakers.

PACEMAKER hardware design assumption, descriptive: this type of assumption specifies hardware-related domain knowledge or requirements that affect the PACEMAKER system's hardware design. For example, special properties of the bipolar system that make it more favourable than the unipolar system are environmental assumptions of this type.

PACEMAKER hardware design assumption, quantitative: this type of assumption specifies implied knowledge or requirements on the hardware design of the PACEMAKER system. For example, the safe levels of energy the PACEMAKER may apply to the heart are environmental assumptions of this type.

10.10 Lesson 10: Develop a documentation convention and use it consistently

The documentation system used in this thesis for the environmental assumptions follows the following convention, where each assumption identified is discussed in three aspects:

1. **Type** – What type of assumption it is.
2. **Significance** – Why it is necessary to document this assumption; what difference would it make not to include this assumption in the documentation.
3. **Relevance** – Its relevance to the original PACEMAKER System Specification, i.e., how does it help to clarify the original document; as well as its relevance to other environmental assumptions of a different category.

10.11 Lesson 11: Allow extension and flexibility of the documentation convention

One attribute all great designs have in common is their ability to anticipate and accommodate change. Accommodating changes is one of the most challenging aspects of good software design. The common areas that are likely to change in a software system include business rules, hardware dependencies, input and output, nonstandard languages features, and difficult design and construction areas. Among

these, *hardware dependencies* is the most relevant to the PACEMAKER project, and should be documented as part of the requirements specification as assumptions.

The foundational, three-element-based documentation convention initially proposed in this thesis was extended at multiple points during the research to include new, additional elements in order to accommodate the needs to document different types of assumptions and their class-specific properties. For example, the likelihood-of-change index was introduced specifically to accommodate the rapid advances in hardware development when documenting hardware related assumptions.

As a result, for instance, information associated with a typical hardware assumption would be documented using the following documentation convention:

Type: PACEMAKER hardware design assumption, descriptive.

Significance: ...

Relevance: Independent missing assumption.

Likelihood of Change: *Likely*.

For the purpose of illustration, this thesis defines two levels of likelihood-of-change:

Likely: the identified hardware assumption is highly likely to change within 12 months;

Not likely: the identified hardware assumption is not likely to change within 12 months.

Furthermore, the proposed documentation convention was again extended to include new elements pertaining to environmental assumptions concerning the system's behaviour.

The base types of environmental assumptions were expanded to include the following types:

(Software) system behaviour assumption, descriptive: this type of environmental assumption documents the desired behaviour the (software) system is expected to act in accordance with. It usually exists in the form of a set of 'rules', which collectively defines the set of actions and responses the system can take under specific environmental conditions. This type of assumption also documents the rationale behind the prescribed behaviour of the (software) system, linking the system characteristics back to the properties of its domain environment. Examples from this category include assumptions on the PACEMAKER's responses to sensed signals during various timing cycles, and the influence of events in one chamber of the PACEMAKER upon the other.

(Software) system behaviour assumption, quantitative: this type of environmental assumptions encapsulates important numerical values in determining the desired behaviour of the PACEMAKER system. Examples from this category include the conventionally accepted durations of various timing cycles.

And again, the proposed documentation convention was further extended in documenting another class of assumptions, namely those concerning the system boundaries **B1.2** and **B1.4**.

The base types of environmental assumptions were expanded again to include the following types:

Magnet assumption: this type of environmental assumption is related to the PACEMAKER's behaviour upon the application of a medical magnet.

Communication assumption: this type of environmental assumption encapsulates important background information characterizing the serial communication between the Device Controller-Monitor and the PACEMAKER's Pulse Generator.

Chapter 11

Conclusion and Future Work

11.1 Conclusion

This thesis presents the research findings of the PACEMAKER project. It documents the procedure used to identify, classify, and document the environmental assumptions that are missing from the original *PACEMAKER System Specification*.

In summary, this thesis answers the following questions:

1. What can be done in order to improve the original *PACEMAKER System Specification* with respect to environmental assumptions?
2. Why is it beneficial, in terms of enhancing software quality, to include the documentation of environmental assumptions – which sometimes are (wrongfully) perceived as being collateral and optional – as part of the software requirements document.
3. How should such environmental assumptions be documented?

More specifically, this thesis

- Presents an abstract model for the PACEMAKER System.
- Identifies system boundaries and interfaces in the PACEMAKER model.
- Identifies environmental assumptions for the PACEMAKER system.
- Presents a classification system for the environmental assumptions identified for the PACEMAKER system based on the proposed model.
- Proposes a process for identifying environmental assumptions.

Furthermore, the research findings presented in this thesis are not limited to the PACEMAKER system. Firstly, the documentation convention proposed in this thesis for the PACEMAKER system's environmental assumptions is meant to be generalized and can be extended to address similar documentation needs posed by all kinds of software systems. Additionally, the process of environmental assumptions elicitation described in this thesis provides a useful reference for conducting similar assumption identification projects. Lastly, the classification system presented in this thesis for the environmental assumptions exhibits one facet of a grander conceptual system – one that incorporates multiple '*views*' of the same set of assumptions, with each *view* being distinguished by a unique set of classification criteria.

In conclusion, the PACEMAKER project is a magnified case study, demonstrating the practicality of the proposed documentation approach, and the way it can be applied to similar real-world problems, to ultimately improve the quality of the software under consideration.

11.2 Future Work

11.2.1 Provide different ‘views’ in rendering the documented assumptions

The classification system presented in this thesis for the environmental assumptions exhibits one facet of a grander conceptual system – one that incorporates multiple ‘*views*’ of the same set of assumptions, with each *view* being distinguished by a unique set classification criteria.

So, the proposed documentation system can be further refined by providing different ‘views’ of the set of assumptions. Examples of such different ‘views’ include:

1. assumptions can be rendered according to whether or not the assumption in question is a ‘(business) rule’.
2. descriptive assumptions vs. quantitative assumptions
3. according to the type of the assumption, i.e., is the assumption Definitive, or is it Necessary Domain Knowledge, or is it a hardware design assumption, etc.
4. assumptions can also be viewed according to their relevance towards the original documentation.

Having such choices of viewing the set of elicited assumptions adds extra dimensions to the proposed documentation system and makes it more practical and flexible to use with different software control systems.

11.2.2 Index of Likelihood of Change

The proposed *index of likelihood of change* element in documenting the environmental assumptions in this thesis can be further developed into a more elaborated indexing system to capture more precise information on the probability of changes on an assumption as well as to provide better adaptive measures towards anticipated changes.

In summary, having such extensive indexing system would help:

1. identify assumptions that seem likely to change,
2. separate assumptions that are likely to change, and
3. isolate assumptions that seem likely to change.

Appendix A

Acronyms

AP Atrial Pace

AS Atrial Sense

ARP Atrial Refractory Period

ATR Atrial Tachycardia Response

AV Atrial-to-Ventricular

BOL Beginning Of (battery) Life

BPM Beats Per Minute

cc Cardiac Cycle(s)

CCI Cardiac Cycle Interval

DCM Device Controller-Monitor

ECG Electrocardiogram, external heart signals **EGM** Electrogram, internal heart signals

EOL End Of (battery) Life

EP Electrophysiology, electrophysiologist **ERN** Elective Replacement Near

ERT Elective Replacement Time

HRL Hysteresis Rate Limit

ICD Implantable Cardio-Defibrillator

IS-1 Industry Standard lead type 1

LRL Lower Rate Limit

MSR Maximum Sensor Rate

NSR Normal Sinus Rhythm

PG Pulse Generator

ppm Pulses Per Minute

PVARP Post-Ventricular Atrial Refractory Period **PVC** Premature Ventricular Contraction

SIR Sensor Indicated Rate

SRD Sustained Rate Duration

URL Upper Rate Limit

VP Ventricular Pace

Bibliography

- [1] Agateller (Anthony Atkielski). *Schematic diagram of normal sinus rhythm for a human heart as seen on ECG*. URL: <http://en.wikipedia.org/wiki/File:SinusRhythmLabels.svg>.
- [2] *The NASPE/BPEG Generic Pacemaker Code for Antibradyarrhythmia and Adaptive-Rate Pacing and Antitachyarrhythmia Devices* 10 (1987).
- [3] Joseph D. Bronzino. *Medical Devices and Systems*. Connecticut, USA: CRC Press, 2006.
- [4] Manfred Broy and Oscar Slotosch. “From Requirements to Validated Embedded Systems”. In: *EMSOFT '01: Proceedings of the First International Workshop on Embedded Software*. London, UK: Springer-Verlag, 2001, pp. 51–65.
- [5] Ties van Brussel. *Anatomy of the Tony Walsh*.
- [6] *Cardiac Pacemaker*. URL: www.wikipedia.com.
- [7] Arthur A. Ciarkowski. *FDA Regulatory Requirements for Medical Devices with Control Algorithms*. 2000.

-
- [8] *Electrophysiology*. URL: <http://www.free-ed.net/sweethaven/MedTech/CardiacRhythm/571.asp?iNum=0102>.
- [9] *Federal Food, Drug and Cosmetic Act*. FDA.
- [10] Roger A. Freedman. “Standard Indications and Contraindications for Pacemaker Implantation: The 1998 ACC/AHA Guidelines”. In: *Cardiac Electrophysiology Review* 2.4 (1999), pp. 353–357.
- [11] Robert Glass. *Software Creativity*. Reading, MA: Addison-Wesley, 1995.
- [12] Graham C. Goodwin. *Control System Design*. Reading, Massachusetts: McGraw-Hill Professional, 2004.
- [13] Gabriel Gregoratos. “Indications and Recommendations for Pacemaker Therapy”. In: *American Family Physician* 71.8 (2005), pp. 1563–1570.
- [14] A.C Guyton and J.E. *Textbook of Medical Physiology*. 11th ed. Philadelphia: Elsevier Saunder, 2006.
- [15] C. L. Heitmeyer. *Software Cost Reduction*.
- [16] Raghbir Singh Khandpur. *Biomedical Instrumentation: Technology and Applications*. Reading, Massachusetts: McGraw-Hill Professional, 2004.
- [17] Nancy G. Leveson, Jon Damon Reese, and M. Per Erik Heimdahl. “Designing specification languages for process control systems: lessons learned and steps to the future.” In: *In Software Engineering—ESEC/FSE*. Springer Verlag, 1999, pp. 127–145.
- [18] Steve McConnell. *Code Complete*. Microsoft Press, 2004.

-
- [19] *MedlinePlus Medical Encyclopedia*. electronically. National Library of Medicine, URL: <http://www.nlm.nih.gov/medlineplus/ency/article/003868.htm>.
- [20] *Pacemaker Formal Methods Challenge*. 2007. URL: <http://sqr1.mcmaster.ca/pacemaker.htm>.
- [21] *Safety of Medical Electrical Equipment, Part-I: General Requirements for Safety*. IEC. 1988.
- [22] *Safety Requirements for Medical Electrical Systems*. IEC.
- [23] A.J. van Schouwen, D.L. Parnas, and J. Madey. “Documentation of requirements for computer systems”. In: *Requirements Engineering, 1993., Proceedings of IEEE International Symposium on* (1993), pp. 198–207.
- [24] *Threshold potential*. 2001. URL: http://en.wikipedia.org/wiki/Threshold_potential.
- [25] unknown. *PACEMAKER System Specification*. Software requirement specification. Boston Scientific, 2007.