



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시. 귀하는 원저작자를 표시하여야 합니다.



비영리. 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지. 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

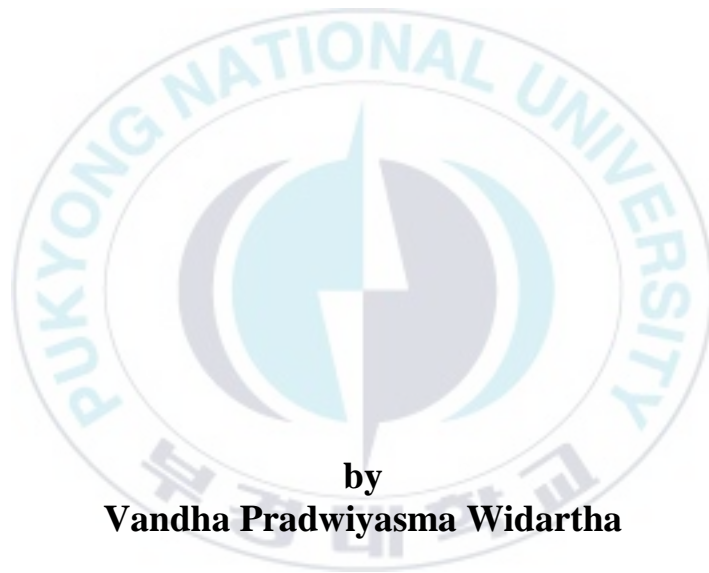
저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

Thesis for the Degree of Master of Engineering

A Study on the Safety Analysis of Safety-Critical Telecardiology Health Care Systems



by
Vandha Pradwiyasma Widartha

**Interdisciplinary Program of Information Systems
The Graduate School
Pukyong National University**

February 2016

A Study on the Safety Analysis of Safety-Critical Telecardiology Health Care Systems

(안전 중요 원격 심장 건강 관리 시스템의 안전성 분석에 관한 연구)

Advisor: Prof. Man-Gon Park

by
Vandha Pradwiyasma Widartha

A thesis submitted in partial fulfillment of the requirements
for the degree of

Master of Engineering

in Interdisciplinary Program of Information Systems, The Graduate School,
Pukyong National University

February 2016

A Study on the Safety Analysis of Safety-Critical Telecardiology
Health Care Systems


A Thesis

by

Vandha Pradwiyasma Widartha

Approved by:


(Chairman) Chang Soo Kim


(Member) Hilwaldi Hindersah


(Member) *Man-Gon Park*

February 26, 2016

Table of Contents

List of Tables	iv
List of Figures	v
Abstract	vi
Chapter 1. Introduction.....	1
1.1 Background	1
1.2 Purpose and Structure of The Thesis	3
Chapter 2. Understanding of Safety Analysis, and Fault Tree Analysis	
Implementation Area and Hazard Analysis Technique	5
2.1 Safety Analysis Method	5
2.1.1 Hazard Analysis.....	6
2.2 Implementation Fault Tree Analysis of the Storage Tanks in The Chemical Industry	12
2.3 A Survey of Safety Analysis Techniques for a Safety Critical Systems.....	15
Chapter 3. Safety-Critical System of Telecardiology Health Care System	19
3.1 System Definition	21
3.1.1 Fatal Accident of Safety-Critical Healthcare System	21
3.1.2 Telecardiology Healthcare System	22
3.1.3 Telecardiology system architecture	24

3.1.4 Telecardiology System Devices	25
3.1.5 The Main Requirements of Developing Telecardiology System	26
3.1.6 Telecardiology System Network Communication	27
3.2 Risk Analysis of Telecardiology System.....	29
3.2.1 Hazard Identification.....	30
3.2.2 Hazard Probability	33
3.2.3 Hazard Evaluation Matrix	34
Chapter 4. Defect Failure of Telecardiology Health Care System Using Fault Tree Analysis	36
4.1 Fault Tree Analysis.....	36
4.1.1 The Rules of Building Fault Tree	39
4.2 The Building Fault Tree Analysis (FTA) of Telecardiology Health Care System	40
4.2.1 Function Block Diagram of Telecardiology Health Care System.....	41
4.2.2 Fault Tree Analysis of Telecardiology Health Care System.....	42
4.3 Qualitative Approach of Fault Tree Analysis or Minimal Cut Set.....	43
Chapter 5. Safety Evaluation of Telecardiology Health Care System	48
5.1 Quantitative Approach of Fault Tree Analysis.....	48
Chapter 6. Conclusion	51
Reference	53
Acknowledgements	58

List of Tables

Table 2.1 Differentiation of Hazard Analysis Types and Techniques	7
Table 2.2 Hazard Analysis Types	8
Table 2.3 Hazard Analysis Techniques	9
Table 2.4 Event in the Fault Tree and Descriptions.....	14
Table 2.5 Comparison of Safety Analysis Technique.....	17
Table 3.1 Telemedicine Services	22
Table 3.2 Telecardiology System Devices Requirements	26
Table 3.3 Hazard Identification Approaches	32
Table 3.4 The High Level Risks of Telecardiology System	32
Table 3.5 Consequence Scale of Health Records on Telecardiology Health Care System.....	34
Table 3.6 Likelihood Scale of Health Records on Telecardiology Health Care System.....	34
Table 3.7 Hazard Evaluation Matrix of Health Records on Telecardiology System	35
Table 4.1 The Symbol and Gate Type of Fault Tree Analysis	37
Table 4.2 The Rules of Fault Tree Analysis Construction.....	39
Table 4.3 Boolean algebra laws	44
Table 4.4 Acronym of Fault Tree Analysis Event	45
Table 4.5 Qualitative Result of Telecardiology Health Care System	47

List of Figures

Figure 2.1 The Procedures of Hazard Analysis	7
Figure 2.2 Fault Tree Analysis Diagram of Fire and Explosion Accident	13
Figure 3.1 Methodology Safety-Critical Telecardiology Health Care System.....	20
Figure 3.2 The Telecardiology System Architecture	24
Figure 3.3 Holter Device.....	25
Figure 3.4 Transferring electrocardiogram from home or ambulance via satellite, telephone network or GSM network.....	28
Figure 3.5 Block Diagram of Telecardiology System Network	29
Figure 3.6 Hazard Identification Steps	31
Figure 4.1 Function Block Diagram of Telecardiology Health Care System.....	41
Figure 4.2 The procedures of Fault Tree Analysis.....	42
Figure 4.3 Fault Tree Analysis Diagram of Telecardiology Health Care System	44
Figure 5.1 Quantitative approach of Fault Tree Analysis Diagram.....	50

안전 중요 원격 심장 건강 관리 시스템의 안전성 분석에 관한 연구

부경대학교 일반대학원 정보시스템학과(협동과정)

요 약

안전성 분석의 작동 메커니즘은 시스템 실패를 유발하는 위험요소들과 같은 모든 위험들을 찾아내는 것이다. 많은 경우에서, 안전성 분석은 위험 감소를 위하여 위험 자체에 대한 이해를 증진시키는 좀 더 체계적인 분석을 사용하게 된다. 안전성 분석은 FTA와 같은 위험 평가 방법으로 위험을 평가하고 발견해 내는 다양한 방법을 가지고 있다.

FTA는 종종 안전성 중요 시스템을 분석하는데 사용이 되고, 이러한 분석기법은 정량적이고 질적으로 우수하게 위험 요소들을 발견해내는 데 널리 사용이 되고 있다. Fault Tree는 논리적이고 그래픽적으로 원하지 않는 사건과 상태를 야기하게 되는 가능한 사건들의 다양한 조합을 나타내게 된다.

이 논문에서는, 안전성 중요 tele-Cardiology 건강 관리 시스템에서 발생할 수 있는 위험 요소들을 평가하고 찾아내기 위하여 FTA를 사용한 안전성 분석을 제안하게 된다. Tele-Cardiology 시스템의 FTA는 최소 cut set을 사용한 질적 분석을 통하여 다양한 tele-Cardiology 시스템을 나타낼 것이고, 정량적인 분석으로부터 나타난 발생 가능성은 tele-Cardiology 건강 관리 시스템이 사용하기에 적절한지 아닌지를 증명할 수 있게 될 것이다.

Chapter 1. Introduction

1.1 Background

Health care system is one of an important part of computer system development. Health care systems are developed with involve organization people, stakeholder or institutions, and resources to deliver health care services to target populations. Health care services should cover several elements such as personal health care services, public health services, teaching and research activities, and health insurance. Health care services can connect or communicate between the patient and doctor, hospital services, and data exchange or electro diagram. The services of health care system include electronic health records, clinical alerts and reminders, and etc [2]. Using health care system is good for improving population health because a good health care system delivers quality services to all people whenever and wherever they need.

The telemedicine is an application of health care service which enables communication among patients, doctor, health specialist and another health workers in remote area. Telemedicine is the use of communication and electronic information technology to support and provide health care when among patient and health experts could not meet each other in the same place and time [27]. Some of telemedicine application is usually used for monitoring health patients using teleconsultation, teleradiology, telecardiology and etc.

Telecardiology is an application of telemedicine that allows the delivery and management of clinical cardiology data using ICT. Telecardiology is utilized for handling and minimizing a cardiovascular sufferers especially for remote area. According to American Heart Association and World Health Organization, “In 2008, cardiovascular deaths represented 30% all global deaths with 80% or those deaths taking place in low and middle-income countries”, for that matter is predicted that a

number of death due to cardiovascular grow to more 0.5% year [28]. The existence of telecardiology systems are used to save time, money, and lives caused by cardiovascular disease. In UK, 29 general practitioners trialed a local telecardiology service. Telecardiology system was demonstrated that out of 24,541 patients assessed by the service, around 65.8% cardiac cases can be prevented by this system. It also was estimated the savings to the National Health Service (NHS) were in excess of £300,000 and ECG reports were provided within 2 hours [29]. However, telecardiology system can lead to be harmful to human, if systems have some failure.

Safety-critical system is one of system whose provide critical information. The critical information such as data which is used to make safety-critical decision, critical data which is stored in computer database and etc. Those data can cause loss of human life, severe injuries, environmental damage and loss of property when those data have faults or errors [3]. There are many well known examples of safety-critical system in application areas such as medical devices, aircraft flight control, weapons, nuclear systems and other systems[4]. Failures of the system especially for telecardiology health care system widely happened on medical error either from human error or system error. Medical error is a serious problems of health care that result human death. In the United States, medical error resulted among 44000 and 98000 America people die per year [6]. Errors have a several types, such as diagnostic, treatments, preventive and technical errors [4]. In telecardiology health care system, system has full responsibility to monitor health activities. The failures of telecardiology system are occurred if there are some defect system functionality especially in logic programming, communication network and incompatibility workflow. This failures can result the doctors or specialist practitioners give a wrong diagnosis so that it endangers patient. For example misapplication a unit of body weight and misapplication a unit of body temperature [5]. The one of ways for overcoming system failures is using hazard analysis or safety analysis.

The working mechanism of safety analysis is find out all risk possibility which can cause hazard on the system failures. Hazards can be identified using safety analysis.

The main concept of safety analysis is to identify and evaluate hazards and safety characteristics [6]. Safety analysis has a several methods for identifying and assessing hazard. The one of method which support to give safety assessment of system hazard is Fault Tree Analysis.

Fault Tree Analysis (FTA) is one of hazard analysis technique or safety analysis method which widely used for identifying hazard qualitatively and quantitatively. Fault tree analysis (FTA) is frequently used for analyzing safety-critical system. FTA is used in many area, such as chemical, mechanical, electrical, nuclear power plants, health care area and etc.

From the issues above, the issues of the medical accident particularly in telecardiology health care systems require serious treatment. Errors or faults should be identified early to prevent undesired event occurrence and assessed to ensure the system is worth to be used or no. In this research, we propose safety analysis using FTA to identify and evaluate failure which can raise hazard on safety-critical telecardiology health care system. We hope through safety analysis using FTA technique can be alternative solution for identifying and assessing safety-critical system.

1.2 Purpose and Structure of The Thesis

The objectives of this thesis is to try and understand safety analysis of safety-critical telecardiology health care system. The technique analysis which is used is fault tree analysis. This will enable us to be able to identify causal dependencies between a hazard on system level and failures of individual components on telecardiology health care system. The analysis uses two kind of approaches, that is qualitative and quantitative approach methods. Qualitative approach method of fault tree analysis is used to focus on determining minimal cut sets for event using boolean algebra laws to identify failure in telecardiology health care system. Whereas, quantitative approach method of fault tree analysis aims to provide estimations about probabilities, rates or severity of consequences to know the telecardiology health care system is safe to be used or no.

The structure of this thesis is broken down into the following modules :

Chapter 1 Introduces the facts of the state of hazards which are occurred on safety-critical system especially on telecardiology health care system.

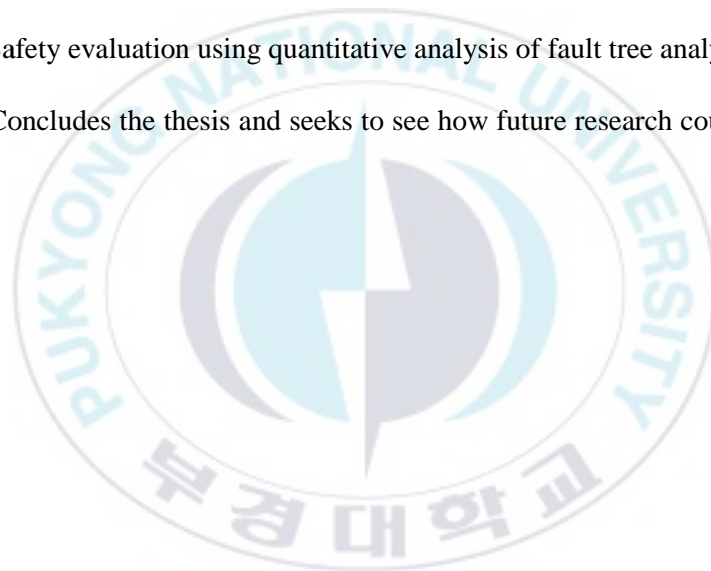
Chapter 2 Understanding of safety analysis, implementation of fault tree analysis and hazard analysis.

Chapter 3 Discusses about how is telecardiology health care system called safety-critical system.

Chapter 4 Analysing the risks of failure that occurred on telecardiology health care system using qualitative analysis of fault tree analysis.

Chapter 5 Safety evaluation using quantitative analysis of fault tree analysis.

Chapter 6 Concludes the thesis and seeks to see how future research could be carried out.



Chapter 2. Understanding of Safety Analysis, and Fault Tree Analysis Implementation Area and Hazard Analysis Technique

2.1 Safety Analysis Method

There are a number of reasons for conducting a safety analysis, which can concern either an existing workplace or a design situation. The basic goal of a safety analysis is to prevent accidents. In most cases, safety analysis has advantages compared with traditional safety work. A deeper and more systematic analysis will improve understanding of risks, which will better support hazard reduction. There are number of advantages in using a defined safety analysis methods. But this presupposes that a suitable method is chosen according to situation, otherwise, utility will be small and perhaps even negative. Using one or several methods of safety analysis may have the following kinds of advantages:

1. A general experience is that far more hazards and ideas for improvements are discovered than in traditional safety work.
2. One part of the explanation for this is that safety analysis offers a complementary perspective and adds to earlier ways of working and thinking.
3. Several methods are based on solid experiences, which have been put together in compact format, with checklists etc. other ways of obtaining the necessary information would be more time consuming and difficult.
4. In complex system, which usually include several hazards, it is essential to work systematically, so that important aspects are not overlooked.
5. Safety in a system depends on co-operation between people in different positions. Using a safety analysis method can give a good format for teamwork because it

offers a step-by-step approach. Even if lengthy discussions should arise, and several meetings are needed, it is possible easily to get back on track.

6. In teamwork, application of a safety analysis method can give a more objective touch to discussions. It has been shown to support inclusion of the experiences of works and operators. It can also be beneficial for discussion of controversial well handled.
7. The application of specified method gives a certain guarantee that safety issues are well handled.
8. The results are documented in a uniform manner.

In generally, safety analysis is a systematic procedure for analyzing systems to identify, evaluate hazards and safety characteristics. Safety analysis has a technique to identify and evaluate hazards. The use of hazard analysis is used for identify hazards.

2.1.1 Hazard Analysis

The hazard analyses are carried out to identify the hazards which can be found in computer system. The hazard analyses examine the whole system such as subsystems, system components, and interrelationships. They also provide inputs to the following National Airspace Integrated Logistics Support (NAILS) elements such as training, maintenance, operational and maintenance environments, and system / components disposal. There are several types in performing a hazard analysis. It shows that figure 2.1.

There are two categories of hazard analyses: types and techniques. Hazard analysis type describes an analysis category, and technique describes a unique analysis methodology. The type specifies analysis timing, depth of detail, and system coverage. The technique refers to a unique analysis methodology that provides specific results. System safety is established upon seven basic types, while there are over 100 different techniques available.

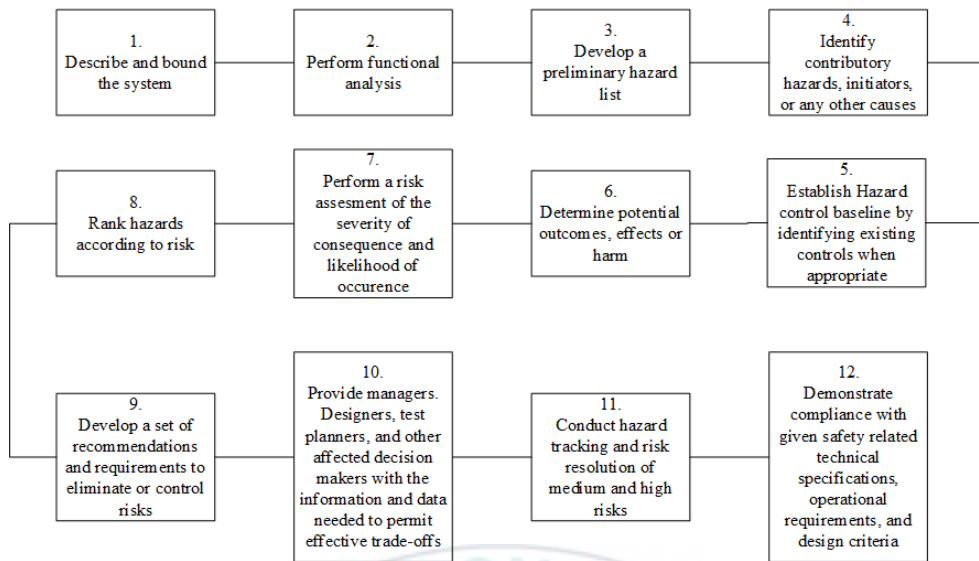


Figure 2.1 The Procedures of Hazard Analysis

In general, there are several different techniques available to achieve each of the various types. The overarching distinctions between type and technique are summarized in Table 2.1. Hazard analysis types describe the scope, coverage, detail, and life-cycle phase timing of the particular hazard analysis. Each analysis type is intended to provide a phase-dependent analysis that readily identifies hazards for a particular design phase in the system development life cycle.

Table 2.1 Differentiation of Hazard Analysis Types and Techniques

Type	Technique
Establishes where, when, and what to analyze	Establishes how to perform the analysis
Establishes a specific analysis task at specific time in program life cycle	Establishes a specific and unique analysis methodology
Establishes what is desired from the analysis	Provides the information to satisfy the intent of the analysis type
Provides a specific design focus	

Each analysis types describe a point in time when the analysis should begin, the detail level of the analysis, the information type available, and the analysis output. The objectives of each analysis type can be achieved by various analysis techniques. The analyst needs to carefully select the appropriate techniques to achieve the goals of each of the analysis types. The analysis types and analysis techniques are shown on table 2.2.

Table 2.2 Hazard Analysis Types

Type	Function
Conceptual Design Hazard Analysis Type (CD-HAT)	To compile a list of hazards very early in the product or system development life cycle to identify potentially hazardous areas. These hazardous areas identify where management should place design safety emphasis.
Preliminary Design Hazard Analysis Type (PD-HAT)	To identify system-level hazards and to obtain an initial risk assessment of a system design. It is performed early, during the preliminary design phase, in order to affect design decisions as early as possible to avoid future costly design changes.
Detailed Design Hazard Analysis Type (DD-HAT)	To evaluate the detailed design for hazards and hazard causal factors and the associated subsystem risk levels.
System Design Hazard Analysis Type (SD-HAT)	To perform a formal analysis for identifying system-level hazards and evaluating the associated risk levels.
Operations Design Hazard Analysis Types (OD-HAT)	To evaluates the operations and support functions involved with the system.
Health Design Hazard Analysis Type (HD-HAT)	To assesses design safety by evaluating the human health aspects involved with the system.
Requirements Design Hazard Analysis Type (RD-HAT)	To establish traceability of safety requirements and to assist in the closure of mitigated hazards.

Hazard analysis technique describes a unique analysis methodology. The technique refers to a specific and unique analysis methodology that is performed following a

specific set of rules and provides specific results. There are over 100 different hazard analysis techniques in existence, and the number continues to slowly grow. Many of the techniques are minor variations of other techniques. And, many of the techniques are not widely practiced. There are 22 of the most commonly used techniques by system safety practitioners. It shows in table 2.3.

Table 2.3 Hazard Analysis Techniques

Technique	Function
Preliminary Hazard List Analysis (PHL)	To identify and list potential system hazards and to identify safety critical parameters and mishap categories
Preliminary Hazard Analysis (PHA)	To analyze identified hazards, usually provided by the preliminary hazard list (PHL), and to identify previously unrecognized hazards early in the system development.
Subsystem Hazard Analysis (SSHA)	To expand upon the analysis of previously identified hazards and to identify new hazards from detailed design information.
System Hazard Analysis (SHA)	To ensure safety at the integrated system level
Operating and Support Hazard Analysis (O&SHA)	To ensure the safety of the system and personnel in the performance of system operation
Health Hazard Assessment (HHA)	To provide a design safety focus from the human health viewpoint and identify hazards directly affecting the human operator from a health standpoint.
Safety Requirements / Criteria Analysis (SRCA)	To ensure that all identified hazards have corresponding design safety requirements to eliminate or mitigate the hazard and that the safety requirements are verified and validated as being successful in the system design and operation.
Fault Tree Analysis (FTA)	To find the root causes of a hazard or undesired event during design development in order that they can be eliminated or mitigated.

Technique	Function
Event Tree Analysis (ETA)	To evaluate all of the possible outcomes that can result from an initiating event.
Failure Mode and Effects Analysis (FMEA)	To evaluate the effect of failure modes to determine if design changes are necessary due to unacceptable reliability, safety, or operation resulting from potential failure modes.
Fault Hazard Analysis	To identify hazards through the analysis of potential failure modes in the hardware that comprises a subsystem.
Functional Hazard Analysis	To identify system hazards by the analysis of functions.
Sneak Circuit Analysis (SCA)	To identify latent paths that can cause the occurrence of unwanted functions or inhibit desired functions, assuming all components are functioning properly.
Petri Net Analysis (PNA)	To provide a technique to graphically model systems components at a wide range of abstraction levels in order to resolve system reliability, safety, and dependency issues.
Markov Analysis (MA)	To provide a technique to graphically model and evaluate systems components in order to resolve system reliability, safety, and dependency issues.
Barrier Analysis	To evaluate these energy sources and determine if potential hazards in the design have been adequately mitigated through the use of energy barriers.
Bent Pin Analysis (BPA)	To identify hazards caused by bent pins within cable connectors.
HAZOP Analysis	To identify the potential for system deviations from intended operational intent through the unique use of key guide words.
Cause Consequence Analysis (CCA)	To identify and evaluate all of the possible outcomes that can result from an initiating event (IE).

Technique	Function
Common Cause Failure Analysis (CCFA)	To identify CCF vulnerabilities in the system design that eliminate or bypass design redundancy, where such redundancy is necessary for safe and reliable operation.
MORT Analysis	To identify those specific design control measures and management system factors that are less than adequate (LTA) and need to be corrected to prevent the reoccurrence of the mishap or prevent the undesired event.
Software Safety Assessment (SWSA)	To evaluate a system and determine if an SWSSP is required and, if so, determine what and how much safety effort is required.

Hazard analysis can be performed in either a qualitative or qualitative method, or a combination of both.

2.1.1.1. Qualitative Analysis of Hazard Analysis Technique

The qualitative analysis is a review of all factors affecting the safety of a product, system, operation, or person. It involves examination of the design against a predetermined set of acceptability parameters. All possible conditions and events and their consequences are considered to determine whether they could cause or contribute to injury or damage. A qualitative analysis always precedes a quantitative one. The objective of a qualitative analysis is similar to that of a quantitative one. Its method of focus is simply less precise. Qualitative analysis verifies the proper interpretation and application of the safety design criteria established by the preliminary hazard study. It also verifies that the system will operate within the safety goals and parameters established by the Operational Safety Assessment (OSA). It ensures that the search for design weaknesses is approached in a methodical, focused way.

2.1.1.2 Quantitative Analysis of Hazard Analysis Technique

The Quantitative analysis takes qualitative analysis one logical step further. It evaluates more precisely the probability that an accident might occur. This is accomplished by calculating probabilities. In a quantitative analysis, the risk probability is expressed using a number or rate. The objective is to achieve maximum safety by minimizing, eliminating, or establishing control over significant risks. Significant risks are identified through engineering estimations, experience, and documented history of similar equipment. A probability is the expectation that an event will occur a certain number of times in a specific number of trials. Actuarial methods employed by insurance companies are a familiar example of the use of probabilities for predicting future occurrences based on past experiences. Reliability engineering uses similar techniques to predict the likelihood (probability) that a system will operate successfully for a specified mission time. Reliability is the probability of success. It is calculated from the probability of failure, in turn calculated from failure rates (failures/unit of time) of hardware (electronic or mechanical). Fault Tree Analysis is one of hazard analysis technique which support both of qualitative and quantitative manner to identify and evaluate system hazard.

2.2 Implementation Fault Tree Analysis of the Storage Tanks in The Chemical Industry

Fault tree analysis was used for analysing harmful factors of the the tanks systematically. As is well known that chemical industry was industry which causes several harmful either for human or environtment such as burning tanks, explosive, toxic substances, and personnel poisoning. Therefore, in this paper, prevention and control of chemical industry tank was so indispensable. One of safety analysis method, that was Fault Tree Analysis (FTA) was used for analysing harmful. In recent development, Fault tree analysis provides a reliable analysis of the safety system. Fault

tree analysis is a logical and diagrammatic method for identifying and evaluating the probability of an accident. FTA is also classified as a powerful technique analysis since it can provide qualitative and quantitative approaches. In addition, to obtain a good analysis result, FTA used boolean algebra law, boolean logical modelling and probability theory. Fault analysis is began with defining top events of this issue. The top event is “tank fire or explosion”. If the top event has determined, the next process was find out all causes about top event which possible occurred. The fault tree diagram is shown as fig 2.2.

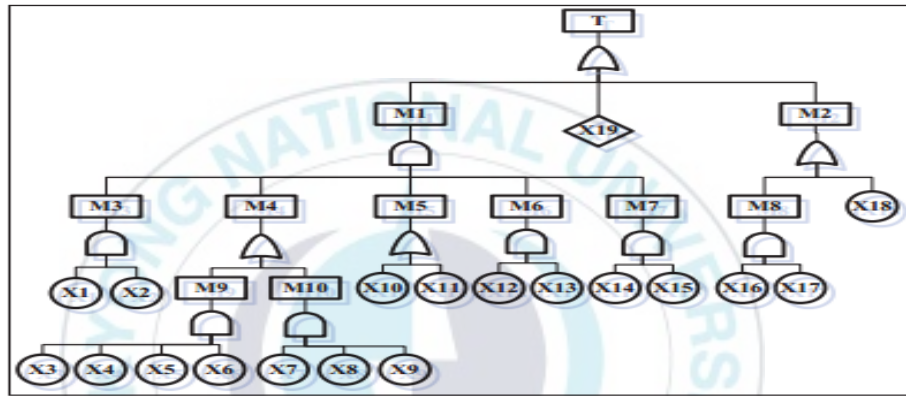


Figure 2.2 Fault Tree Analysis Diagram of Fire and Explosion Accident

Qualitative analysis approach of this method was utilized to identify what kind of factors which caused top event occurrence. The final steps of qualitative analysis approach was determining the number of minimum cut sets of fault tree analysis. In this research was resulted as many 38 minimum cut sets. Whereas quantitative analysis was utilized for assessing the top event probability. Top event probability was calculated using equation of the probability of any gate.

To “AND” gate, the equation was :

$$P(G_i) = \prod_{j=1}^n q_j = q_1 \cdot q_2 \dots q_n \quad (1)$$

To “OR” gate, the equation was :

$$P(Gi) = 1 - \prod_{i=1}^n (1 - qi) = 1 - (1 - q1) \cdot (1 - q2) \dots (1 - qn) \quad (2)$$

From calculating probability, probability of top event was $0.0028 = 1 \text{ time} / 357.14 \text{ year}$. It meant that if the probability of basic event in the accurate and sable condition, the explosion of this isseu can be happened one time per 357 years [20].

Table 2.4 Event in the Fault Tree and Descriptions

Event	Description	Event	Description	Event	Description
T	Fire and explosion accident of storage tank	M10	Bad grounding	X10	Not wearing anti-static clothing
M1	Sources of ignition	X1	Smoking	X11	The friction work
M2	Explosive mixed gas	X2	Use fire	X12	Black metal collision
M3	Open flame	X3	Liquid flows fast	X13	Friction between shoes and ground
M4	Electrostatic discharge by storage tank	X4	Pipe wall roughness	X14	Direct lightning stroke
M5	Electrostatic discharge by person	X5	The friction of air and liquid	X15	Lightning induction
M6	Mechanical spark	X6	Measurement errors	X16	Unqualified tank
M7	Lightning discharge	X7	Without grounding device	X17	Device not having regular inspection
M8	Tank leakage	X8	Grounding resistance is not required	X18	Poor ventilation
M9	Accumulation of static electricity	X9	Grounding lines damage	X19	Above the explosion limit

2.3 A Survey of Safety Analysis Techniques for a Safety Critical Systems

Safety-critical system is critical system which result in some serious injury, severe damage, loss of human lives, environment destruction and etc. A safer system is so highly required especially in IT industry. It has been proven by there are so many demands of safer system. In this research, explain about the kind of technique analysis for analysing critical system. There are two type of analysis techniques, that is formal and informal techniques. Formal techniques concern on academic research because these techniques have highly prospect for ensuring safe systems. Whereas informal techniques are usually called by traditional techniques. In addition, combination among formal and informal techniques are used for safety analysis in this research. The analysis techniques that are used both formal and informal such as FHA (Fault Hazard Assessment, FTA (Fault Tree Analysis), FMEA (Failure Mode Effect Analysis), FSSA (Facility System Safety Analysis), and DCCA (Deductive Cause Consequence Analysis).

Informal techniques use several technique for identifying system failure that cause hazard. Each techniques have their own way to identify hazard. The first technique is FMEA or FMECA (Failure Mode Effect Critical Analysis). FMEA is a bottom up approach which used for classifying error that may cause hazards for user. It strongly helpful to propose changes during in system development process. Success of FMEA can be seen on how detail understanding of the whole system. Functional Failure Mode Effect Analysis (FFMEA) can be used independently to success and complete analysis of safety-critical systems. The second technique is FTA. FTA is conventional technique of fault tree using top down approach which is used for finding all errors from root cause of these hazards. The success of FTA is dependent on the creativity and imagination of the analyst. It focuses on failures that don't have roots and failures on redundancy works. One of advantages of FTA is it can combine qualitative and quantitative evaluation to avoid accidents. The third technique is FHA. FHA use

Hazard Analysis and Operability (HAZOP) basic concepts. HAZOP concerns on identifying errors that may occur in design of development system so that these errors can be minimized. The fourth technique is Petri model. It uses backward analysis to determine critical areas of the system using fault tolerant or fail-safe system mechanisms.

Formal techniques are techniques which thoroughly study for safety critical system. Several techniques which are used in formal techniques include FTA, FMEA, DCCA, UML, FSSA and MUC. Formal fault tree is used for verifying completeness and weakness analysis that may occur since informal fault tree is removed. FTA approach can declare a system either system has safe or less safe. For example, there are two events, if any events have failure, system will failure. FTA and FMEA can be used for initial analyzing minimal critical sets for DCCA. Existence of an empty as critical sets prove that there is weakness of system functional and system design inappropriate. DCCA concerns on functional correctness of the system. The main reason is functional property can be more rigorous verified through formal method. Another technique of formal technique is UML (Unified Modelling Language). UML can be used for analyzing safety and can be integrated with other safety technique either from formal or informal technique. The one part of UML is use case. Use case is used to initial analysis through diagram and to decrease failure mode of the system using MUC (Misuse case). Table 2.6 shows comparison of safety analysis technique [24].

Table 2.5 Comparison of Safety Analysis Technique

Parameters	HAZOP	FTA	FMEA	FMECA	CORAS	DCCA	MUC	FSSA
Risk identification	Security aspects are focused	Top Down Approach	Bottom Up Approach	FMEA of critical part	Integrated informal approach	Empty, Single and Multi failure Mode, Minimal Critical set of failure modes	Misuse cases to analyze behavior	Addresses primary failure and rule out hidden failures
Risk Analysis	Used as input for other techniques	Major events are analyzed	Minor errors that may occur are evaluated	Critical parts are analyzed and mitigated	A combinatorial effort for informal techniques	Minimal Critical set of failure modes	Addresses misbehavior	Hidden and complete set of failure modes is discovered through formal check
Risk Evaluation	Used to evaluate other techniques	Can be evaluated with some criteria	Can be evaluated with some criteria	Can be evaluated with some criteria	A combinatorial effort for informal techniques	Compare with Criteria	Unintended Behavior to find flaws	Compare with non failure sensitive specification
Risk Treatment	Multiple options are identified	Can be Prioritized	Can be prioritized	Alternative to critical parts are identified	A combinatorial effort for informal techniques	Addresses Criticality Set	Addresses unintended behavior	Completeness of the system
Automation	No	Yes	Yes	Yes	No	No	Semi-automated	No
Formalization of Approach	Not Possible	Possible	Possible	Possible	Semi-Formal	Already Formal Method	Semi-Formal	Already Formal Method
Skills of	Software	Creative	Creative	Creative	UML , Software	Creativity ,	UML,	Formal Methods

Parameters	HAZOP	FTA	FMEA	FMECA	CORAS	DCCA	MUC	FSSA
Analyst	Skills	and Imagination	and Imagination	and Imagination	Skills, Creativity	Formal Methods	Creativity and Imagination	and Informal Approaches
Components, Languages or Artifacts Used	Functional and Operational Specification	Fault Trees	Fault Trees	Fault Trees	Fault Trees , Use Cases	CTL and Automata	Misuse Cases, Fault Trees	Fault Trees, State Charts and Automata
Risk Identification	Security aspects are focused	Top Down Approach	Bottom Up Approach	FMEA of critical part	Integrated informal approach	Empty, Single and Multi failure Mode, Minimal Critical set of failure modes	Misuse cases to analyze behavior	Addresses primary failure and rule out hidden failures

Chapter 3. Safety-Critical System of Telecardiology Health Care System

This chapter deals about safety-critical system of telecardiology health care system. As known that safety-critical system has several phases to determine the system is categorized as safety-critical system or no. In system safety theory, risk analysis is used to analyze hazards that can be occurred in those system. Risk analysis of this research includes define system, hazard identification, hazard probability and hazard evaluation matrix. Within defining system, the first thing performed is finding out accident that occurred in health care system to understand the influence of hazards for human life. Defining system comprises system description, system architecture, system devices, system requirement standard, and system network communication. After completing system definition, hazard identification is performed to figure out hazards and failures which occurred in the system. Hazard probability is used for recognizing about possible number of incidents per year is reached. Hazard probability will be described into table based on the rule of thumb and hazard

Evaluation matrix is performed to categorize hazard level after identifying hazard. By knowing hazard identification, hazard probability and hazard evaluation matrix, the risks of telecardiology health care system can be known as references to be analyzed in hazard analysis using Fault Tree Analysis (FTA). Since FTA requires Function Block Diagram (FBD) to identify and complete its analysis, then those risks will be considered and used in FBD to identify what kind of failure in telecardiology health care system. FTA uses both

qualitative and quantitative approaches. The detail methodology of this research can be seen in fig. 3.1

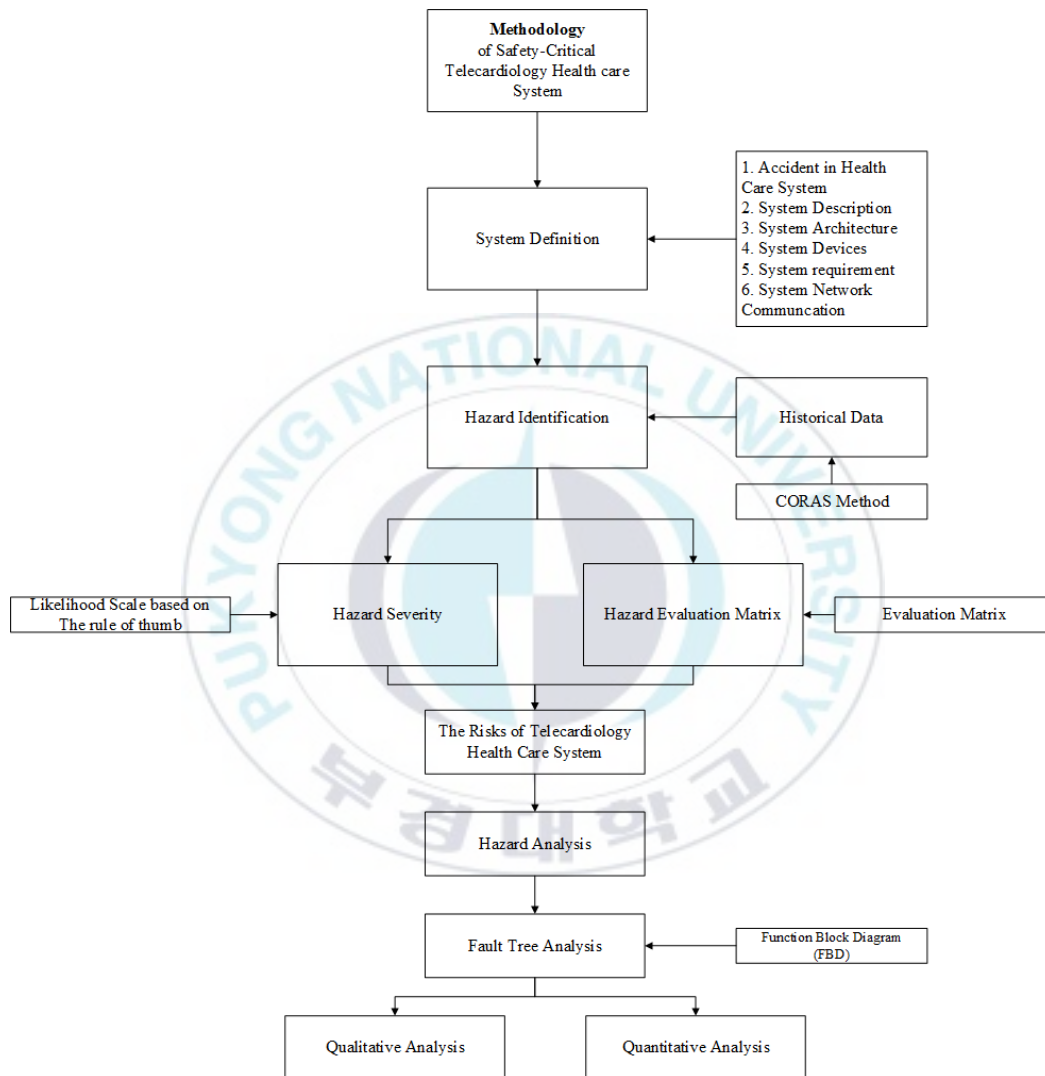


Figure 3.1 Methodology Safety-Critical Telecardiology Health Care System

3.1 System Definition

3.1.1 Fatal Accident of Safety-Critical Healthcare System

Therac-25 was a radiation therapy machine which categorized in safety-critical system of healthcare system or health informatics. Therac-25 was used for curing the cancer patients. It had been successfully performed around 20.000 irradiations on the region's cancer patient's [30]. The usual treatment of this machine sent out a dose of around 200 accepted measurement radioactive energy (rads) such as x-ray. Design of this machine offered two modes of radiation therapy as in the following [31]:

1. Direct electron-beam therapy, which sent out doses of high energy (5MeV to 25 MeV) electrons over short periods of time.
2. Megavolt X-ray therapy, which sent out X-rays resulted by colliding high energy (25 MeV) electrons into a target patient.

Therac-25 machine was performed on direct electron-beam therapy mode when a low powered electron beam was flashed directly from the machine, then deployed to safe concentration using scanning magnets. Whereas on megavolt X-ray mode, the machine was designed to rotate four components within the path of the electron beam. A target which is converted the electron beam into X-rays, a flattening filter was deployed the beam out over a larger are, then a collimator formed the X-Ray beam and ion chamber which measured by the strength of the beam. However this machine is very helpful for patients especially for cancer patients. This machine was be able to endanger patient's even patient death.

In January 1987, there were accidents of the use of therac-25 in Washington. The accidents was occurred since found system malfunction or errors that indicating the incorrect dose had been sent out to the patients. The malfunction system caused therac-25 machine producing higher dose of electron beam (over 100 times as great as during treatment) in spite off target absent so that it caused human death [32].

3.1.2 Telecardiology Healthcare System

Telemedicine systems are one of health care service system which can help monitoring human health routinely. They use telecommunication and information technology to deliver clinical health care at a distance. Some services of telemedicine are integrated electronic health record, diagnosis by phone, diagnosis by video call, and etc in real-time as shown in table 3.1. Telemedicine systems are included a type of safety-critical systems. Communication protocol quality among user and service provider in telemedicine system is very important to the success of a telemedicine system. Therefore if telemedicine systems have a fault and failure either in operate system or in human error, they can result hazard for human life.

Table 3.1 Telemedicine Services

Telemedicine Service	Description
Real-time consulting	this services assist a patient in primary care physician a distance
Telemonitoring	Collecting patient data using Wearable Devices and sending the data to a healthcare, monitoring agency for remote testing and diagnosis. it also includes personalized alerts that inform a patient's healthcare provider in times of physical/mental trauma
Telesurgery	Allowing the surgeon to perform an operation on a patient from a distant location
Remote medical education	Facilitatiing medical education to the health care service community and targeted groups from a geographically different location
Telehealth data service	Sharing specialized health information with the other Health service providers, the education industry, research firms, and the government agencies etc.

Telemedicine Service	Description
Videoconferencing	Consultation media between patient and doctor using transmission if digitized video images.
Telecardiology	One of the application branches of telemedicine that transmits cardiac data such as ECG, radiographs, ultrasounds and medical records from the patient site to cardiologist.

Telecardiology is an application of telemedicine that enables the delivery and management of clinical cardiology data through the use of ICT. The use of telecardiology is used to facilitate cardiologist and general practitioners (GP) within interpret electrocardiogram (ECG) through telephone transmission. The telecardiology service consists of ECG interpretation detected, assessment of critical case and therapy recommendation. Using telecardiology can help general practitioners, doctors to diagnose and control cardiac or heart disease acute or chronic since it provides ECG checkup to detect risk factors of patient whose have risk factors of cardiac disease early. Among the most common applications of telecardiology, there is the possibility of recording an electrocardiogram, through mobile devices, and transmitting it in real time to a service center for specialist reporting, storage and subsequent analysis.

Telecardiology internet base development has been used since 2008 [33]. The telecardiology delivers electrocardiogram (ECG) signal and echocardiography image with telecommunication technologies such as Satellite, Edge, UTMS, LTE, etc. In modern technology, telecardiology enables for reliable remote ECG interpretation. It uses electrical device using 12-leads which is implanted on human body. In this research, telecardiology application will be used is electrical device using 12-leads and using wireless technology for communication system.

3.1.3 Telecardiology system architecture

The rapid technology development especially for electronics and telecommunication systems have influenced the society in overcome issues innovatively. It enables to process and deliver many vital parameter of the human body at distance. Using a specialized hand-held (electronic devices), the device is implanted on human body, and it encodes the ECG into the sound. The sound is decoded electronically and displayed a full 12 –leads ECG on screen at the Cardiac Monitoring Centre. ECG data will be sent via internet to the server center in real time. In the server center, patient ECG data will be stored through patient database and analyzed in the Cardiac Monitoring Centre. Health operator, doctor (specialist) and patient can communicate each other to give diagnose of cardiac patient via internet immediately. Within minutes, an oral report is going to be sent out to the patient via telephone. A complete written report is delivered to doctor and patient using email or fax. The result of investigation ECG patients is stored securely and intended as comparator among old data and new data of the same patient. The telecardiology system can be describe on figure 3.2.

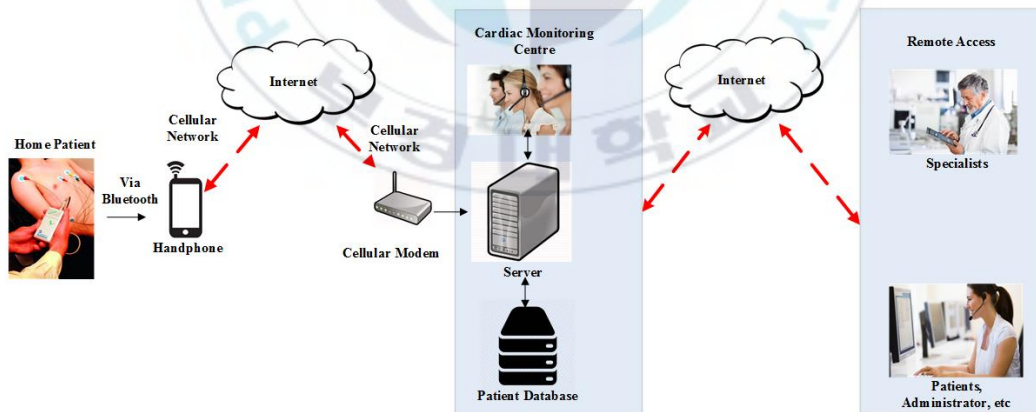


Figure 3.2 The Telecardiology System Architecture

3.1.4 Telecardiology System Devices

Telecardiology system devices can deliver ECGs to a service center for displaying, reporting and archiving their ECGs data. These devices must be certified how to use them. It means that a specific design with proper instructions must be performed by the manufacturer so that the intended users can use those device safely and effectively. There are some device that commonly use for telecardiology system such as home devices, professional devices, holters, wearable devices, and etc.

3.1.4.1 Holters Monitoring System

Holters are the other class of devices whose a reduced quality with respect to diagnostic ECGs due to they have a frequency response from 0.5 up to 40 Hz compared to diagnostic ECGs with 0.05 up to 150 Hz bandwidth. It means that, holters have capacity to monitor electrical heart for 24 hours. These devices can transmit data to a service center and enable remote cardiologist to monitor patients.

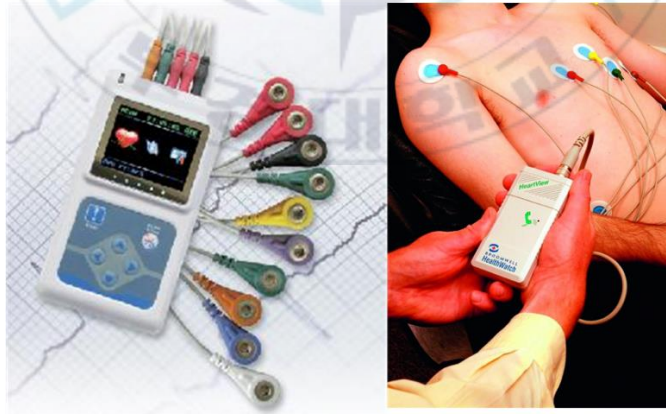


Figure 3.3 Holter Device

3.1.5 The Main Requirements of Developing Telecardiology System

Telecardiology is developed using single-lead-telephone electrocardiograms system (TTEM) to monitor patient's cardiac for the first time. At present, telecardiology system uses workstation to deliver 12-leads electrocardiograms between remote health care unit via telephone or computer network. Workstations have main functions, such as record and send electrocardiograms, echocardiograms, heart murmurs, sounds, vocal messages and pictures. Developing telecardiology system require main requirement, technical specifications as shown in table 3.3.

Table 3.2 Telecardiology System Devices Requirements

Requirement	Spesification
Event Holter ECG Recording	12- Leads
Frequency Range	0.05 Hz – 100 Hz
CMRR	>70db
Patient Cable	10 electrodes
Transmission	Acoustic, not automatic
Modulation	FM tone
Recording Period	41 s
Transmission Period	43 s
Input Dynamic Range	± 5 mV
DC offset correction	± 300 mV
Carrier Frequency	1700 Hz
Frequency Deviation	100 Hz / mV

The European Committee for Standardization (CEN) has defined the Standard Communications Protocol for Computer-Assisted Electrocardiography to assist the inter-

connectivity of different system. It includes eleven sections, such as patient data / ECG acquisition data, Huffman tables used in encoding the ECG data, ECG lead definition, QRS location, encoded median data, residual signal or encoded rhythm data, global measurements, textual diagnosis for the interpretation device, manufactured specific diagnosis and over reading data, lead measurement results, and statement codes resulting from the interpretation [12].

3.1.6 Telecardiology System Network Communication

Telecardiology require the robust network communication system to transmit ECG data to the cardiologist (specialist), doctor and patient. In the telecardiology development, telecardiology has used several technologies started from analog to digital to transmit data. The transmission of the clinical/ECG data is performed using traditional analog trans-telephonic systems via the public switched telephone network (PSTN) or using digital communication via the usual IP networks (xDSL, GPRS, UMTS, satellite networks, etc.) [25]. Telephones have been used for auscultating (method of physic checkup hearing heart and breath sounds) for over 70 years [35]. ECG tracings can be delivered via fax for consultation or second opinion to a distant medical specialist. In Fig. 3.4 shows a telecardiology system based on different modes of telecommunication mode such as telephone network, GSM network or satellite. Interactive systems for live interactive consultations offer an efficient and effective alternative to provide diagnostic and confirmatory consultations in telecardiology. Since telecardiology is more often interview structured involving physical examination, inspectio of spesific locations on the body of abnormal findings indication poor cardiac function, particularly with reference to auscultation of body structures including the heart, lungs, arteries, and abdomen. Therefore, technical issues like bandwidth, video input devices assumed great importance.

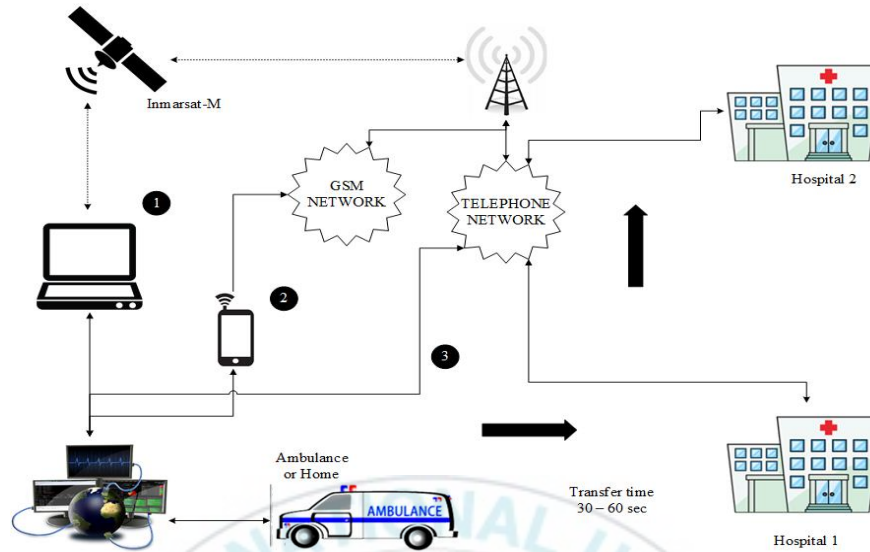


Figure 3.4 Transferring electrocardiogram from home or ambulance via satellite, telephone network or GSM network.

Due to this research uses home devices for telecardiology system. The network communication in which appropriate is mobile network communication [38]. The system network communication consists the portable ECG acquisition (holter) connected to patients. The base stations (BS) receives information. The GPRS communication protocol to transmit the continuous ECG with a minimum delay, the GSM voice channel to allow a specialist to establish a direct call and the internet access to a database host center to monitor patient from their home. The database system module saves the patient records along with their ECGs and other relative information including all the fields that requires at the appropriate format such as clinical treatment, symptoms, etc. The block diagram of network can be seen in fig. 3.5

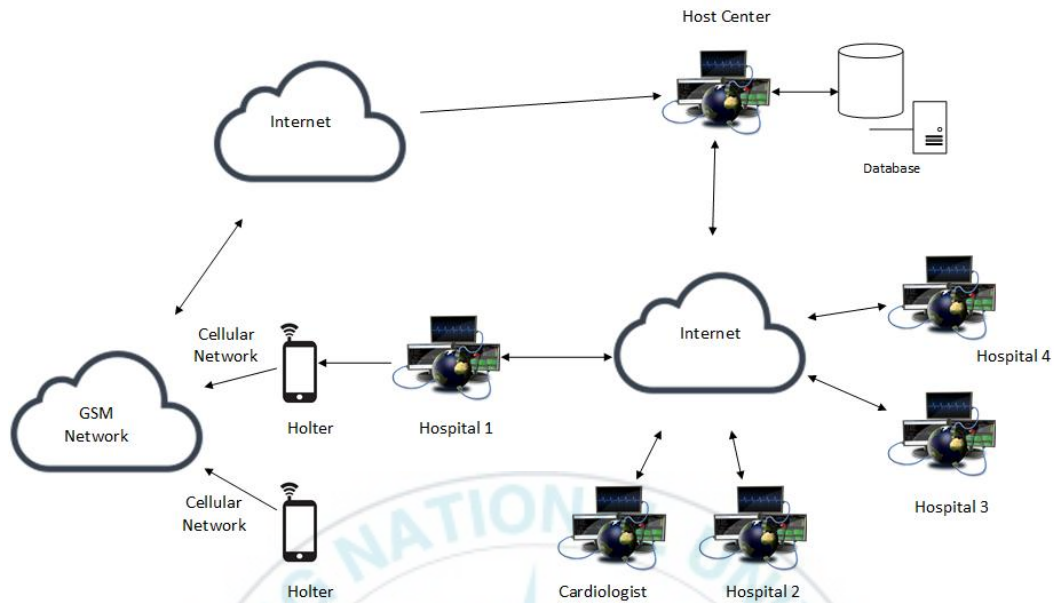


Figure 3.5 Block Diagram of Telecardiology System Network

3.2 Risk Analysis of Telecardiology System

Risk is the possibility of threats from the hazard that become a main source of risk. A hazard is an action which can cause harm not only for human but also for environment. Each system definitely has the risks. In essence, the risks of system are influenced by several factors such as hardware, software and human error. The risks can cause the system cannot work properly, if the system has malfunction or mishap, it can endanger user and damage relate to property. The risks can be minimized by performing risk analysis. The risk analysis is the analysis technique to determine level of risk by analyzing the fundamental components and elements of risk. The risk analysis process focuses on resolving three basic questions, such as what can go wrong and how it can occur?, what is the likelihood that it will go wrong?, and what are the consequences if it does go wrong?

[36]. The risk analysis provides the several basic methods and techniques which interrelated each other, that is hazard identification, risk assessment, determining the significance of a risk, and communicating risk information. In this research, risk analysis is used to identify and assess risks on the telecardiology health care system.

3.2.1 Hazard Identification

Hazard identification is the first method of risk analysis to determine whether the risks are categorized as the cause harm to human life and environment or the risks are categorized as low risk. Hazard identification is a process for identifying hazards and associated events which have the potential to result in a significant consequence. The system is identified thoroughly through the several steps. The steps is shown as figure 3.6.

From the fig. 3.6, the first step for identifying hazard is defining scope or the boundaries of the system which will be analyzed. In determining scope, it may assist to divide the facility into three parts, it includes manageable sections, areas or activities for the hazard identification process. The hazard identification process can only identify hazards that come within scope of the system description. The system description describes about the whole system in detail. Hazard identification methods are classified into 3 generic approaches as shown in table 3.4

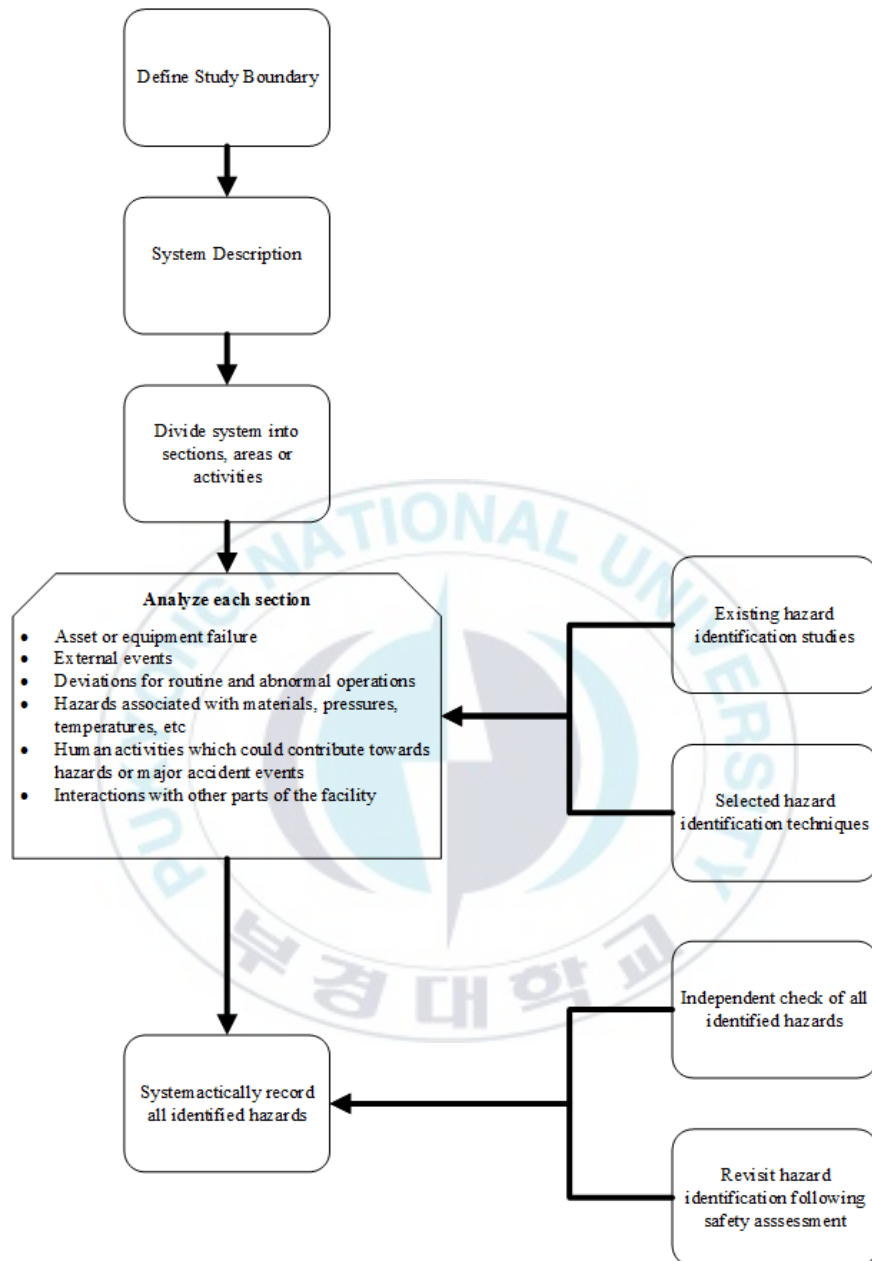


Figure 3.6 Hazard Identification Steps

Table 3.3 Hazard Identification Approaches

No	Approaches	Description
1.	Historical data	Using and analyzing of the existing hazards logs and accident/ incident reports. It also identifies hazard from other risk assessment processes on other systems which might be similar with system.
2.	Brainstorming	Planned and organized sessions aimed at encouraging a team of participants of various relevant experience and expertise to explore the system for potential hazards in a creative way.
3.	Systematic	This method is involving a thorough sequential review of a system using system diagrams to helm focus on the types of failures to be assessed. Systemic hazard identification processes include : <ul style="list-style-type: none"> • Failure Modes Effects and Criticality Analysis (FMECA) • Hazard and Operability Analysis (HAZOP)

In this research, historical data is used for identifying hazard of telecardiology health care system. Historical data is taken by previous research using CORAS method to analyze threat in telecardiology service [37]. Historical data was obtained through brainstorming with involved Representative of General Practitioner, Regional hospital, Health minister and IT manager. Brainstorming resulted high level risk as shown in table 3.4 The risks focused on health records of telecardiology system.

Table 3.4 The High Level Risks of Telecardiology System

The Cause	Incident	The Possibility
Hackers	They break into the system and steal patient's health records	Insufficient security
Employee	Sloppiness compromises confidentiality of patient's health records	Insufficient training

The Cause	Incident	The Possibility
Eavesdropper	Eavesdropping on dedicated connection	Insufficient protection of connection
System failure	System goes down during examination	Unstable connection / immature technology
Network failure	Transmission problems compromises integrity of medical data	Unstable connection / immature technology
Employee	Health records leaks out by accident, compromises their confidentiality and damages the trust in the system	Possibility of irregular handling of health records
Employee	Sloppiness compromises integrity of health record	Prose-based health records

3.2.2 Hazard Probability

A risk is considered to be the probability of an event occurring and consequential impact of the event upon the asset or value. After the risks or hazards are identified by hazard identification, the hazards were assessed to describe their probability of occurrence. The probability of occurrence is an estimate of how often a hazard event occurs. Each hazard of concern is rated in accordance with the numerical ratings. From previous study, the analyst initiate the discussion by suggesting a scale of likelihood based on the following rule of thumb. The rule of thumb means the incident likelihood can called “rare” is set to be maximum one occurrence during the target’s lifetime, the remaining intervals have an increasing number of expected events until the maximum possible number of incidents per year is reached. Because incidents may have different impact depending on which risk is harmed. Table 3.5 shows consequences scale and table 3.6 shows likelihood scale of the risks of health records on telecardiology health care system.

Table 3.5 Consequence Scale of Health Records on Telecardiology Health Care System

Consequence Value	Description
Catastrophic	1000+ health records (HRs)
Major	100 – 1000 HRs
Moderate	10-100 HRs
Minor	1-10 HRs
Insignificant	No HRs

Table 3.6 Likelihood Scale of Health Records on Telecardiology Health Care System

Likelihood Value	Description
Certain	Five times or more per year
Likely	Two to five times per year
Possibly	Once a year
Unlikely	Less than once per year
Rare	Less than once per ten years

3.2.3 Hazard Evaluation Matrix

Hazard evaluation matrix helps to determine acceptable or unacceptable the risks. This matrix provides a tool to evaluate the hazards. It means that a rule is defined for how hazards are going to be evaluated. In application to a specific hazard, Hazard evaluation matrix is described as a table with categories of consequences in rows and categories of likelihood in columns. From historical data, hazard evaluation matrix of health records on telecardiology system is described on table 3.7.

Table 3.7 Hazard Evaluation Matrix of Health Records on Telecardiology System

Consequence / Likelihood	Consequence				
Likelihood					
Rare	Insignificant	Minor	Moderate	Major	Catastrophic
Unlikely	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Possible	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Likely	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Certain	Unacceptable	Unacceptable	Unacceptable	Unacceptable	Unacceptable



Chapter 4. Defect Failure of Telecardiology Health Care System Using Fault Tree Analysis

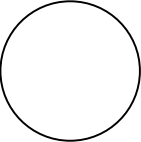
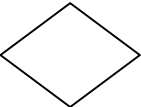

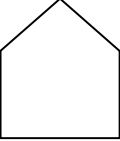

4.1 Fault Tree Analysis

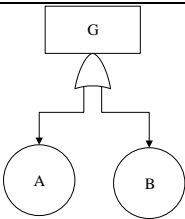
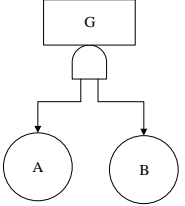
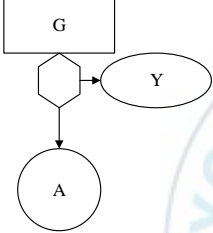
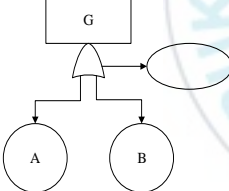
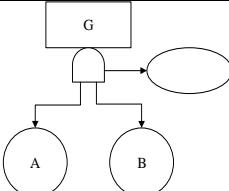
Fault tree analysis (FTA) is a systems analysis technique used to determine the root causes and probability of occurrence of a specified undesired event. FTA is employed to evaluate large complex dynamic systems in order to understand and prevent potential problems. Using a rigorous and structured methodology, FTA allows the systems analyst to model the unique combinations of fault events that can cause an undesired event to occur. The undesired event may be a system hazard of concern or a mishap that is under accident investigation. A fault tree (FT) is a model that logically and graphically represents the various combinations of possible events, both faulty and normal, occurring in a system that lead to an undesired event or state. The analysis is deductive in that it transverses from the general problem to the specific causes. The FT develops the logical fault paths from a single undesired event at the top to all of the possible root causes at the bottom. The strength of FTA is that it is easy to perform, easy to understand, provides useful system insight, and shows all of the possible causes for a problem under investigation.

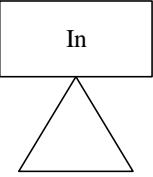
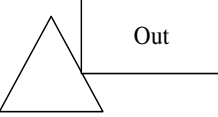
FTA uses analysis qualitatively and quantitatively. Qualitative analysis of FTA is used to figure out which part of system has failure so that the system require to be improved and prevented based on the existing failure to avoid the same thing occurred. Quantitative analysis of FTA is used to know how the probability of undesired event occurred. If the result approaches 1, then system require to be improved or maintained which parts of failure from qualitative analysis. Reducing the failures of probability result, systems are going to well to be used.

To analyze system failures using FTA, first step is building function block diagram of the system to understand how the system works. The next step is building fault tree with symbols which has determined in fault tree analysis theory as described on table 4.1.

Table 4.1 The Symbol and Gate Type of Fault Tree Analysis

Symbol	Gate Type	Description
Event Symbol		
	Basic Event / Primary Event	Basic failure which no need to find out its cause
	Undeveloped Event	A specific failure event which no need to find out its cause either not quite touch or not information available related to failure
	Conditioning Event	A condition specific constraints which are implemented to gate
	External Event	An event which is desired appear normally and not include in failed event
	Intermediate Event	This event contains an event which appear from combination of failed inputs event that enter to gate
Gate Symbol		

Symbol	Gate Type	Description
	OR Gate	OR gate is used for showing that the output occurs only if at least one of the inputs occurs
	AND Gate	AND gate is used for showing that the output occurs only if all of inputs occur together
	Inhibit Gate	This gate shows that the output occurs only if the input event occurs and the attached condition is satisfied
	Exclusive OR Gate	This gate shows that the output occurs if either of the inputs occur, but not both. The exclusively statement is contained in the condition symbol
	Priority AND Gate	This gate shows that the output occurs only if all of the inputs occur together, and A must occur before B. the priority statement is contained in the condition symbol
Transfer Symbol		

Symbol	Gate Type	Description
	Triangle-In	Triangle in or transfer-in is point where sub-fault tree can be begun as continuation to transfer-out
	Triangle out	Triangle out or transfer out is point where fault tree divided to sub fault tree

4.1.1 The Rules of Building Fault Tree

A fault tree analysis has the rules to construct fault tree. Construction of fault tree is described on table 4.2.

Table 4.2 The Rules of Fault Tree Analysis Construction

Rules	Description
Rule 1	The fault event state as a fault. It includes the description and time of a fault state at some particular time
Rule 2	There are two basics types of fault, that is state of system and state of component
Rule 3	If the fault is state of system, fault may use an AND, OR, or INHIBIT gate or no gate at all. To determine which gate to use, there are two ways : <ul style="list-style-type: none"> a. Minimum necessary and sufficient fault events b. Immediate fault events
Rule 4	If the fault is state of component, fault always uses an OR gate. State of those fault events are : <ul style="list-style-type: none"> a. Primary failure is failure of that component within the design envelope or environment b. Secondary failures are failures of that component due to excessive environments exceeding the design environment.

Rules	Description
	c. Command faults are inadvertent operation of the component because of a failure of a control element.
Rule 5	Put an event statement among any two gates
Rule 6	Normal system operation may be expected to occur when faults occur
Rule 7	In an OR gate, the input doesn't cause output. If any inputs exists, the output exists. Fault events under the gate may be a restatement of the output events
Rule 8	In an AND gate defines a causal relationship. If the input events coexist, the output is produced.
Rule 9	An INHIBIT gate describes a causal relationship between one fault and another, but the indicated condition must be present. The fault is the direct and sole cause of the output when that specified condition is present. Inhibit conditions may be faults or situations, which is why AND an INHIBIT gates differerent

4.2 The Building Fault Tree Analysis (FTA) of Telecardiology Health Care System

Within constructing FTA, the first step which should be performed is using functional block diagram (FBD). The FBD represents a simplified representation of the system design and operation for understanding. The FBD shows the subsystem interfaces and the component relationships, moreover the FBD also shows the function which should be performed by the system for successful operation. Based on historical used data which is shown in chapter 3, sending ECG data is very important for patient and cardiologist or doctor to diagnose patient so the FBD of telecardiology Health Care System can be shown as fig. 4.1.

4.2.1 Function Block Diagram of Telecardiology Health Care System

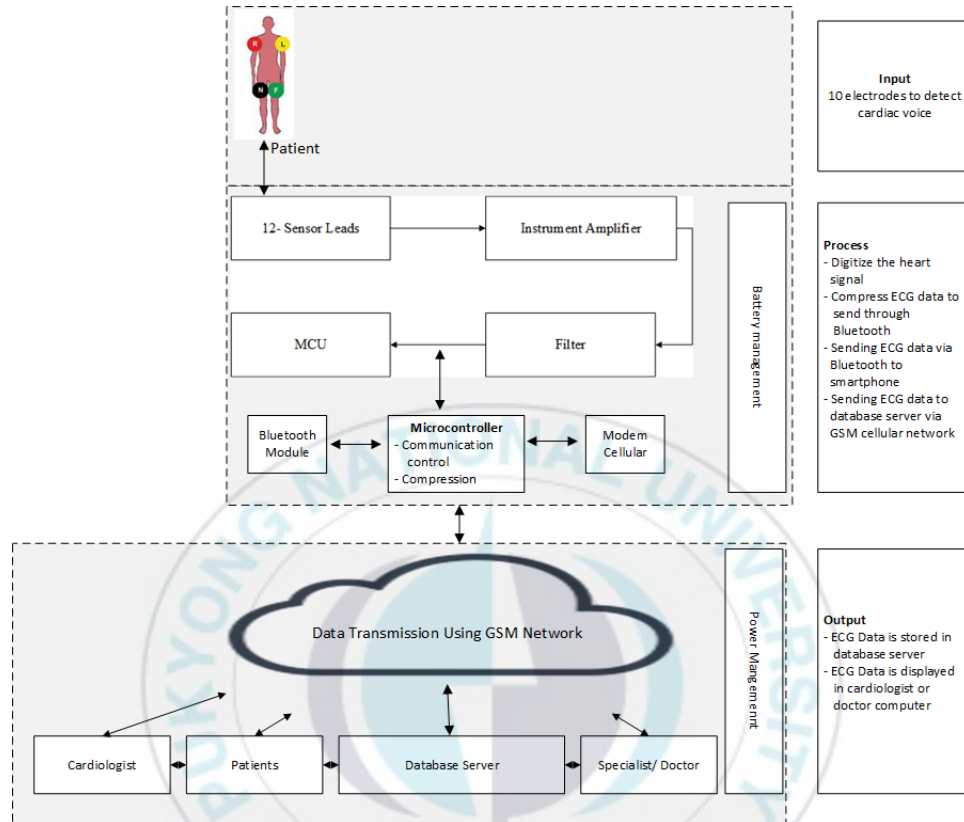


Figure 4.1 Function Block Diagram of Telecardiology Health Care System

From fig. 4.1, The telecardiology holter devices is implanted in human body. The holter device uses 10 electrodes for 12-leads sensor. The holter will result voice signal which compressed in microcontroller to get ECG data. The ECG data is sent to mobile phone via Bluetooth by the help of Bluetooth module paired in microcontroller. The ECG data will be delivered into database server using GSM network communication. The specific

cardiologist or the doctor can see the patient ECG data and diagnose whether the patient cardiac is classified danger or no.

4.2.2 Fault Tree Analysis of Telecardiology Health Care System

Constructing a fault tree analysis should be follow the general procedures of fault tree analysis construction. There are 5 steps in fault tree analysis procedures as described on fig. 4.2

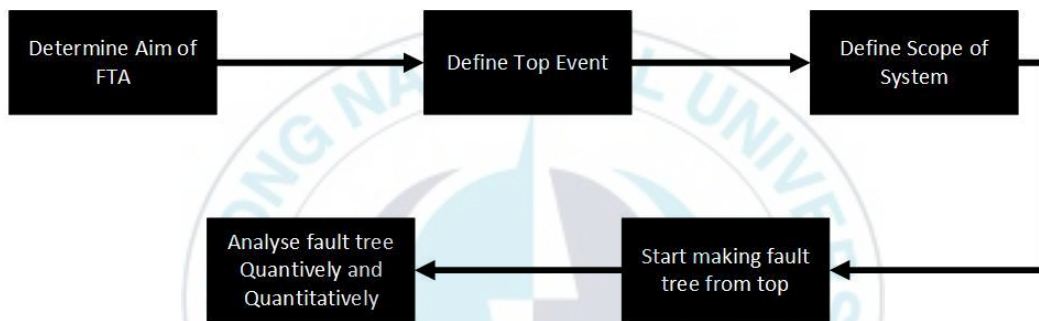


Figure 4.2 The procedures of Fault Tree Analysis

- Step 1. Determining Aim of FTA.

The FTA of this system goal is to figure out the causes of failure on sending the right electrocardiograph data of telecardiology health care system.

- Step 2. Defining Top Event.

Due to initial condition from system is patient delivers electrocardiograph data to cardiologist or doctor using telecardiology system, then we will choose the top event is failure on sending the right electrocardiograph data.

- Step 3. Defining Scope from system.

In the first step will be defined usability and objectivity of this system, physics restriction, analytic restriction and initial state of the telecardiology health care system.

- Step 4. Constructing fault tree from the top.

In this step, fault tree will be investigated what kind of event which can result top event occurrence.

- Step 5. Analyze fault tree qualitatively and quantitatively.

To analyze both qualitative and quantitative analysis from fault tree. The first thing that should be found is minimal cut set. After finding minimal cut set, qualitative analysis will obtained failures that address to top event occurrence directly and quantitative analysis will obtained top event occurrence probability using probability theory. The figure 4.2 shows the detail of fault tree analysis diagram of telecardiology health care system.

4.3 Qualitative Approach of Fault Tree Analysis or Minimal Cut Set

Qualitative approach is approach method procedures that don't require to calculate probability value for each event in logic system. Qualitative approach tends to handle the problem on basic level and to identify relationship between events from logic gate network without quantification. An important factor of qualitative approach determines the minimal cut sets (minimum event causes top event). In The logic gate network theory, the logic gate has two gates commonly used, that is AND gate and OR gate. AND gate is equal multiplication and OR gate is equal addition.

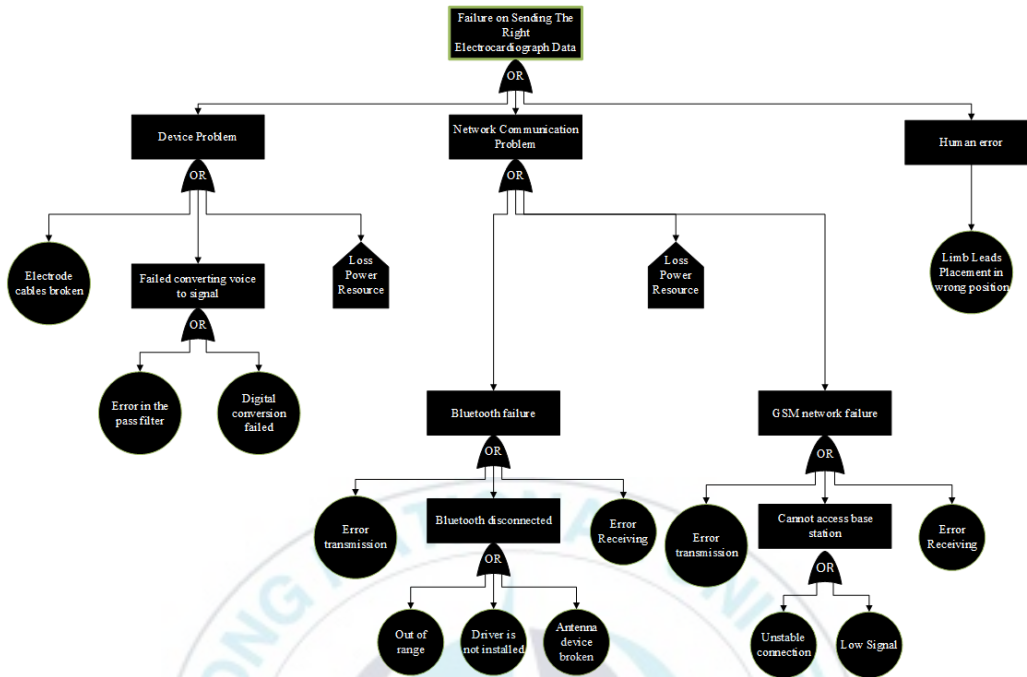


Figure 4.3 Fault Tree Analysis Diagram of Telecardiology Health Care System

Minimum cut sets can be obtained with using Boolean algebra concept which is described in table 4.3.

Table 4.3 Boolean algebra laws

Boolean algebra	Boolean Algebra Laws
$ab = ba$ and $a+b = b+a$	Commutative law
$(a+b)+c = a+(b+c) = a+b+c$	Associative law
$(ab)c = abc$	Associative law
$a(b+c) = ab+ac$	Distributive law
$a*a = a$ and $a+a = a$	Idempotent law

Boolean algebra	Boolean Algebra Laws
$a+ab = a$ and $a(a+b) = a$	Law of absorption

Cut a set is the set of basic event where if all basic the event appeared, there will be a top event. At least cut a set is a combination of the smallest of the set of basic event where if basic the event occurred, will cause a top event occurred. The following will be described finding at least cut set with using method of Boolean algebra. OR gate is the joint of the event and corresponded with the operation of addition of Boolean algebra, whereas the AND gate is a gate that stated a wedge from events and corresponded with the multiplication of Boolean algebra. The first step, define any acronym on each gate and event to ease process of analysis. the acronyms and definitions describe on table 4.4.

Table 4.4 Acronym of Fault Tree Analysis Event

Acronym	Definition	Acronym	Definition
T	Failure on sending the right electrocardiograph data	B2	Error in the pass filter
Ev1	Device problem	B3	Digital conversion failed
Ev2	Network communication problem	B4	Error transmission
Ev3	Human error	B5	Error receiving
Ev4	Failed converting voice to signal	E1	Loss of power resource
Ev5	Bluetooth failure	B6	Out of range
Ev6	GSM network failure	B7	Driver is not installed
Ev7	Bluetooth disconnected	B8	Antenna device broken
Ev8	Cannot access base station	B9	Unstable connection

Acronym	Definition		Acronym	Definition
B1	Electrode cables broken		B10	Low signal
			B11	Limb leads placement in wrong position

- The description of Acronym

T is Top Event || B is Basic Event || E is External Event || Ev is Intermediate Event

From fig. 4.3 and table 4.4. The minimum cut sets can be obtained through Boolean equation below :

$$\begin{aligned}
T &= Ev1+Ev2+Ev3 \\
&= (B1+Ev4+E1)+(Ev5+E1+Ev6)+B11 \\
&= (B1+(B2+B3)+E1)+((B4+Ev7+B5)+E1+(B4+Ev8+B5))+B11 \\
&= (B1+(B2+B3)+E1)+((B4+B6+B7+B8+B5)+E1+(B4+(B9+B10)+B5))+B11 \\
&= B1+B2+B3+E1+B4+B6+B7+B8+B5+B4+B9+B10+B5+B11 \\
&= B1+B2+B3+E1+B4+B6+B7+B8+B5+B9+B10+B11
\end{aligned}$$

So the minimal cut set from fig. 4.3 will be [B1], [B2], [B3], [B4], [B5], [B6], [B7], [B8], [B4], [B10], and [B11].

Qualitative analysis is to get a combination of failure that causes a top event on a system or at least cut set itself. The result qualitative approach of fault tree analysis of telecardiology health care system with top event failure on a system telecardiology is shown on table 4.4.

Table 4.5 Qualitative Result of Telecardiology Health Care System

No	Failures on Cardiology System Failure
1	Electrode cables broken
2	Error in the pass filter
3	Digital conversion failed
4	Error transmission
5	Error receiving
6	Out of range
7	Driver is not installed
8	Antenna device broken
9	Unstable connection on GSM network failure
10	Low signal on GSM network failure
11	Limb leads placement in wrong position

By knowing the cause of failure on sending the right electrocardiogram data of telecardiology health care system from minimum cut set, those failures can be predicted and repaired immediately when those system cannot work properly.

Chapter 5. Safety Evaluation of Telecardiology Health Care System

5.1 Quantitative Approach of Fault Tree Analysis

Quantitative approach is performed for estimating the probabilities of events that will be investigated. Quantitative approach of FTA give specific benefits, however it requires basic concept about probability. Top event can be represented as combination from minimum cut set. So, the probability of top event can be estimated using addition from probability on any cut sets. This approximation type apply if basic event probabilities less than 0.1, it is called event approximations. The fault tree analysis diagram on fig. 4.3 describes that each events are independent. So that the probability of basic event can be assumed as 0.01 and another event can be assumed as 0.001. The probability of failure on each events are as follows on table 5.1 and the probability of top event calculation can be seen in figure 5.1 in detail.

Table 5.1 The Probability of Event

Event	Description	Probability
B1	Electrode cables broken	0.01
B2	Error in the pass filter	0.01
B3	Digital conversion failed	0.01
B4	Error transmission	0.01
B5	Error receiving	0.01
B6	Out of range	0.01
B7	Driver is not installed	0.01
B8	Antenna device broken	0.01

Event	Description	Probability
B9	Unstable connection	0.01
B10	Low signal	0.01
B11	Limb leads placement in wrong position	0.01
E1	Loss of Power Resource	0.001

Minimum cut set which is obtained from qualitative analysis is [B1], [B2], [B3], [B4], [B5], [B6], [B7], [B8], [B4], [B10], and [B11]. So, from the probabilities of basic event, The probability of top event will be:

$$\begin{aligned}
 T &= B1+B2+B3+E1+B4+B6+B7+B8+B5+B9+B10+B11 \\
 &= (0.01+0.01+0.01+0.001+0.01+0.01+0.01+0.01+0.01) + (0.01+0.01)+0.01 \\
 &= 0.071 + 0.02 + 0.01 \\
 &= 0.111
 \end{aligned}$$

So, The probability of failure on sending the right electrocardiogram data of telecardiology health care system is 0.111. The probability theory mentioned that if there is event equal 0, the event will not be occurred. Whereas, if there is event equal 1, the event will be occurred. In this case the result shows that the telecardiology health care system appropriate to be used because the result among 0 and 1 so that the possibility of failure on the telecardiology health care system fairly tiny.

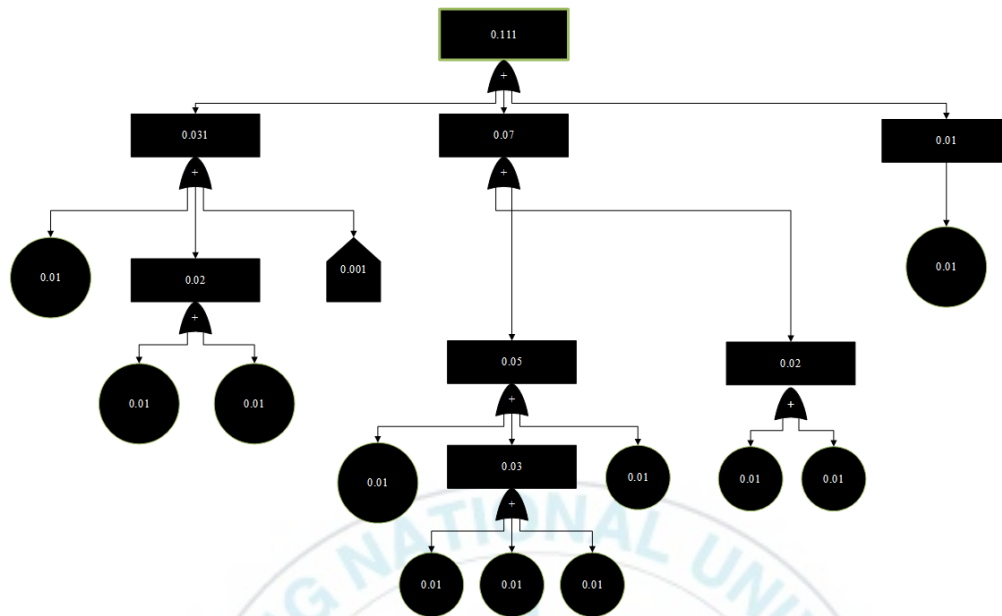


Figure 5.1 Quantitative approach of Fault Tree Analysis Diagram

Chapter 6. Conclusion

Mostly telemedicine devices are categorized as safety-critical system, especially for telecardiology system. Telecardiology system is an application of telemedicine that enables the delivery and management of clinical cardiology data through the use of ICT. The use of telecardiology is used to facilitate cardiologist and general practitioners (GP) within interpret electrocardiogram (ECG) through mobile cellular. Since telecardiology is the one of safety-critical system, those system can result hazard for human life. Therefore, safety analysis is required for identifying hazards that can be occurred on telecardiology health care system. The basic goal of a safety analysis is to prevent accidents. In most cases, safety analysis has advantages to reduce the risks. Safety analysis has a technique to identify and evaluate hazards. The one of safety analysis technique which can be used for analyze hazard is fault tree analysis (FTA).

FTA can identify and predict the hazard in spite of the system accidents never occurred before. Developing fault tree is begun from determine an objective. The goal of fault tree usually relate to failure events from system which will be analyzed. The undesired event of the system is called top event. Top event is a top part of fault tree structure. Afterwards, determining initial state and constraints of system. From top event, start figuring out what kind of failures cause. This failure is called basic event. If every branches from top event is basic event, so developing fault tree has finished.

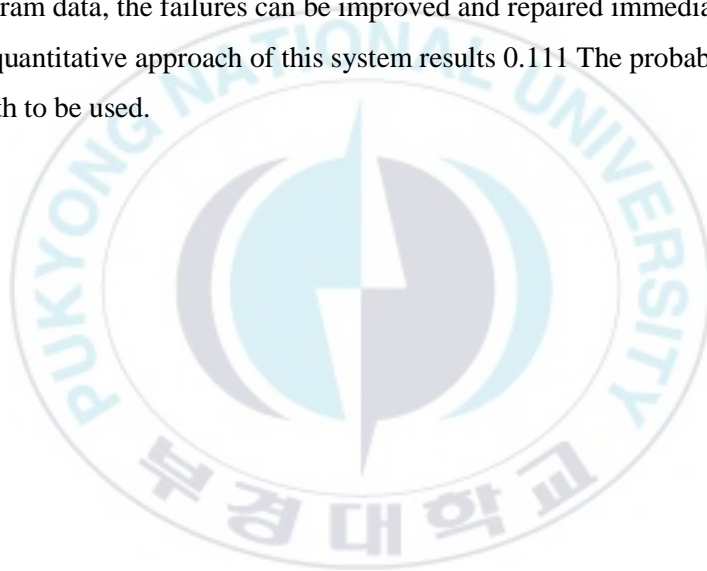
FTA is performed to obtain minimum cut set from basic event of system, if they are occurred so top event will be occurred definitely. The minimum cut set is performed on qualitative approach of FTA.

Fault tree uses symbols which show relationship among failure event. The symbols include event symbols, gate symbols, and transfer symbol. Gate symbols equals with in the Boolean

algebra operation and probability theory in fault tree, so that fault analysis of system using fault tree is able to use Boolean algebra and probability theory.

Minimal cut set is obtained from Boolean expression which is presentation of fault tree. Boolean expression is simplified with Boolean algebra identity. Qualitative approach result from telecardiology health care system has 11 failures. It includes electrode cables broken, error in the pass filter, digital conversion failed, error transmission, error receiving, out of range, driver is not installed, antenna device broken, unstable connection on GSM network failure, low signal on GSM network failure, and limb leads placement in wrong position. It means that if there is failure on telecardiology system especially on failure sending electrocardiogram data, the failures can be improved and repaired immediately.

The result of quantitative approach of this system results 0.111 The probability shows that system is worth to be used.



Reference

- [1]. M. Elena, et al, “Design of a Mobile Telecardiology System Using GPRS / GSM Technology”, Proceedings of the Second Joint, Vol.3, October 2002.
- [2]. L. Chadwick, E.F. Fallon, W.J. Vander Putten, “Functional Safety of Health Information Technology”, Health Informatics Journal, vol. 18 no. 1 36-49, America, March 2012.
- [3]. Knight, John C, “Safety Critical Systems: Challenges and Directions”. ICSE 2002, Proceedings of the 24rd International Conference, Orlando, USA, May 2002.
- [4]. L. T. Kohn, J. M. Corrigan, M. S Donaldson, “To Err Is Human Building A Safer Health System”, Commiteee on Quality of Health Care in America, Institute of Medicine, Washington D.C, USA, 2000.
- [5]. S. Bowman, MJ, Rhia, CCS, Fahima, “Impact of Electronic Health Record Systems on Information Integrity : Quality and Safety Implications”, Online Research Perspectives in Health Information Management, October 2013.
- [6]. L. H. Ringdahl, “Guide to Safety Analysis For Accident Prevention”. IRS Riskhantering AB. Stockholm, Sweden, 2013.
- [7]. M. H .Kim, W. Toyib, M. G. Park, “An Integrative Method of FTA and FMEA For Software Security Analysis of A Smart Phone”, Journal of Korea Multimedia Society, Vol.2, No.12, pp.541-552, January 2013.

- [8]. T. Wulandari. "Analisa Kegagalan Sistem dengan Fault Tree," FMIPA-UI, Depok, Indonesia, 2011.
- [9]. A. M. Burhan, "Fault Tree Analysis As A Modern Technique For Investigating Causes Of Some Construction Project Problems", Journal of Engineering, Vol. 16, No. 2, June 2010.
- [10]. W. A. Hyman, E. Johnson, "Fault Tree Analysis of Clinical Alarms", Journal of Clinical Engineering, Texas A&M University, June, 2008, accessed on 24th August 2015.
http://thehtf.org/documents/FTA_of_Clinical_Alarms-Hyman_and_Johnson.pdf.
- [11]. B. P. Douglass, "Analyze System Safety Using UML Within The IBM Rational Rhapsody Environment", IBM Software Group, Germany, June 2009.
- [12]. M. S. Chowdhury, Md.H. Kabir, K. Ashrafuzzaman, K.S. Kwak, "A Telecommunication Network Architecture for Telemedicine in Bangladesh and Its Applicability", International Journal of Digital Content Technology and its Applications, Vol 3, No 3, September 2009.
- [13]. J. Bai, B. Hu, Y. Zhang, D. Ye, "Communication Server for Telemedicine Applications", IEEE Transactions on Information Technology in Biomedicine, vol. 1, no. 3, september 1997.
- [14]. R. Karimi, N. Rasmussen, L. Wolf, "Qualitative and Quantitative Reliability Analysis of Safety Systems", MIT Energy Laboratory Electric Utility Program, Massachusetts, USA, May 1980.
- [15]. J.S Chitode, "Consumer Electronics", Technical Publications Pune, India, March 2007.

- [16]. H. Azucena, E. Rios, R. D Pena, J. Diaz, “Design and Implementation of a Simple Portable Biomedical Electronic Device to Diagnose Cardiac Arrhythmias”, Elsevier B.V, Sensing and Bio-Sensing Research No. 4 ,Vol.1–10, 2015.
- [17]. M.E. Jennex, “Managing Crises and Disasters with Emerging Technologies Advancements”, IGI Global, United States of America, 2012.
- [18]. I.Y. Chen, C.C. Huang, “A Service-Oriented Agent Architecture to Support Telecardiology Services on Demand”, Journal of Medical and Biological Engineering, No.25(2), Vol.73-79, January 2005.
- [19]. O.F. Roca, M.S. Iudicissa, “Handbook of Telemedicine”, IOS Press, Amsterdam, 2002.
- [20]. A. Hongguang, “Fault Tree Analysis of The Storage Tanks in The Chemical Industry”, Fourth International Conference on Instrumentation and Measurement, Harbin, China, September 2014.
- [21]. Z.A. Abecassis, L.M. McElroy, R.M. Patel, et al, “Applying Fault Tree Analysis TO The Prevention of Wrong-Site Surgery”, Journal of Surgical Research, Vol.193, January 2015.
- [22]. K.L Kam, V. Ramane, C.Y. Ooi, “Development of Platform-Independent Web-Based Telecardiology Application for Pilot Case Study”, IEEE Conference on Biomedical Engineering and Sciences, December 2014.
- [23]. M. Pandey, “Engineering and Sustainable Development: Fault Tree Analysis”, University of Waterloo Press, Waterloo, Canada, 2005.

- [24]. A.A. Haider, A. Nadeem, "A Survey of Safety Analysis Techniques for Safety Critical Systems", International Journal of Future Computer and Communication, Vol. 2, No. 2, April 2013.
- [25]. C. Becchetti, A. Neri, "Medical Instrument Design and Development from Requirements to Market Placements", JohnWiley & Sons Ltd, United Kingdom, 2013.
- [26]. B. Jonathan. V. Stavridou, "Safety-Critical, Formal Methods and Standards", Software Engineering Journal, December 1992.
- [27]. M. J. Field, "A Guide to Assessing Telecommunications in Health Care", National Academy Press, Washington DC, USA, 1996.
- [28]. D. Mozaffarian, et al, (2014, Desember 17), "Heart Disease and Stroke Statistics at A Glance", Retrieved from https://www.heart.org/idc/groups/ahamapublic/@wcm/@sop/@smd/documents/downloadable/ucm_470704.pdf
- [29]. W. Backman, D. Bendel, R. Rakhit, "The Telecardiology revolution: improving the management of cardiac disease in primary care", Journal of The Royal Society of Medicine, vol. 103, No. 11, November 2010.
- [30]. B.W. Rose, 1994, "Radiation Deaths Linked to AECL Computer Errors", retrieved from <http://www.ccnr.org/>.
- [31]. N.G Leveson, C.S Turner, "An Investigation of Therac-25 Accidents", Computer, vol.26, no. 7, pp. 18-41, July 1993.

- [32]. J. Jacky, "Safety-Critical Computing: Hazards, Practices, Standards, and Regulation", Academic Press, Washington, 1996.
- [33]. K.Nikus, V. Virtanen, S. Sclarovsky, M. Eskola, "The Role of Standard 12-Lead ECG in a Telecardiology Consultation Service", Telemedicine and Applications, InTech. 2011.
- [34]. W. Backman, D. Bendel, R. Rakhit, "The Telecardiology Revolution: Improving The Management of Cardiac Disease in Primary Care", Journal of Royal Society of Medicine, No. 442-446, Vol. 103 (11), November 2010.
- [35]. S. Maheshwari, P. Kumar, S. Seshadiri, (2014, April 02), "Telecardiology : A Solution whose Time Has Come", Retrieved from http://www.researchgate.net/publication/280254112_Telecardiology
- [36]. B. M. Ayyub, "Risk Analysis in Engineering and Economics", CRC Press, USA, 2014.
- [37]. F.D. Braber, et al, "The CORAS Model-based Method for Security Risk Analysis", SINTEF, Oslo, 2006.

Acknowledgements

(감사의 말씀)

I want to first of all thank to Allah for all the blessing and strength that He has given me to complete this course and my Master Thesis. This would not be easy to solve without support from all PKNU professors, lectures, Korean friends, foreigner friends, and Indonesian friends, SEAMOLEC, ITB professors and others. So, on this occasion, I would like to express appreciation to all who help, support, and give the best spirit to me so that I was able to accomplish study abroad.

Firstly, I would like to express my sincere gratitude to my advisor Prof. Man-Gon Park for the continuous support my Master study and related research, for his patience, motivation, and immense knowledge. His guidance helped me in all the time of research and writing of this Master Thesis I could not have imagined having a better advisor and mentor for my Master study.

Besides my advisor, I would like to thank to Dr. Myeong Hee Kim, for her advice remarkable, a new knowledge and sharing. Her guidance helped me to grow knowledge intellectually which I have often benefitted from him during course work.

I would like to thank the rest of my Master Thesis committee members: Prof. Chang Soo Kim, Prof. Kyung Hyune Ree, Prof. Bong Kee Shin from Pukyong National University and Dr. Hilwaldi and Prof. Charmadi from Institute Technology of Bandung, for their insightful comments and encouragement, but also for the hard questions which incented me to widen my research from various perspective.

My sincerely thanks also goes to Dr. Gatot Priowirjanto, Dr. Abe Susanto, and Mrs. Cahya who give great opportunity and as the pioneer bridging the Dual Degree Program between

Pukyong National University South Korea and Institute Technology of Bandung Indonesia through abroad scholarship.

I also would like to express my gratitude to ITB Rector, Dean of STEI, and ITB lectures who support and advice which very useful to me even though we discussed online.

I thank to my fellow lab mates: Mr. Bright Gameli Mawudor who give remarkable and beneficial advice, Ms. Kim So Young who help me everything relate to academic and non-academic activity, Mr. Rafal Olenski, Mr. Sung Jin, Mr. Sang, Mr. Young Jo, Ms. Diena Rauda, Ms. Nurul Azhany and other members of Software Engineering and Multimedia Information Systems (SEMI) Lab, in for stimulating discussions, for the sleepless nights we were working together before deadlines, and for all the fun we have had in the last 1 year.

I specially thank my Dual Degree Program colleagues and friends: Mr. Rafinno Aulia, Mr. Sandi Rahmadika, Mr. Heri Arum, Ms. Kadek Restu Yani, Mr. Taufiq Syahrir, Mr. Fairuz Iqbal Maulana, Ms. Siti Witty Ariyanti, Ms. Wibby Aldriani, Mr. Ahmad Wisnu Mulyadi, Mr. Maisevli harika, and Ms. Kokoy Siti Komariah, for their sharing, motivation, and kinship during study in South Korea.

Finally, and most importantly, I wish to thank to my parents, brother, sister-in law, niece, nephews, my beloved sister and her family and also all of my family members for their endless love, encouragement and supporting me spiritually throughout writing this thesis and my life in general.