Development of a PSA-based Safety Assessment and Management Framework for a Nuclear-based Hydrogen Generation System

by

Hai Tang

A Thesis Submitted in Partial Fulfillment

of the Requirements for the Degree of

Master of Applied Science

in

Electrical and Computer Engineering

Table of Contents

Table of Contents ii

Acknowledgement vi

List of Tables vii

List of Figures viii

List of Symbols x

List of Nomenclature xi

1 Introduction 1

1.1 Background of Research 1

1.2 Motivation of Thesis 3

1.3 Objective of Thesis 4

1.4 Organization of Thesis 5

2 Literature review 6

2.1 PSA in Nuclear Power Industry 6

2.1.1 Safety VS Reliability 6

2.1.2 Overview of PSA in Nuclear Power Industry 7

2.1.3 Three PSA Levels 8

2.1.4 PSA in Canadian NPP 9

2.2 Safety Instrumented System and Functional Safety 12

2.2.1 IEC 61508 Standard 13

2.2.2 SIL Assessment 16

2.3 Safety Management in Nuclear-based Hydrogen Generation 19

2.3.1 Cooper-Chloride (Cu-Cl) Thermochemical Cycle.....19
2.3.2 Other Thermochemical Cycles 21
2.3.3 Summary of Safety Studies in Nuclear-Based Hydrogen Generation .23
2.4 Summary of Literature Review.....26
3 PSA-based Safety Assessment and Management Framework.....28
3.1 Overview of PSA-Based Integrated Framework for Safety Management.....29
3.2 Hazard and Risk Identification 32
3.3 Fault Tree Analysis 35
3.3.1 Overview of FTA Methodology 35
3.3.2 FTA Symbols and Mathematical Basis.....36
3.4 Event Tree Analysis (ETA) 38
3.5 Layer of Protection Analysis (LOPA) 40
3.6 SIL Assessment.....43
3.6.1 Analytical Approach and Simplified Equations 45
3.6.2 Software Reliability for SIS.....47
3.7 Summary of the PSA-based Framework.....54
4 Safety Assessment Result 55
4.1 Risk and Hazard Identification 55
4.2 PSA for LOCA.....57
4.2.1 Heat Exchanger System 59
4.2.2 FTA for LOCA 61
4.2.3 ETA for LOCA 65
4.3 PSA for Hydrogen Accidents.....68
4.3.1 Hydrogen Accidents Overview.....70
4.3.2 FTA for Hydrogen Accidents 71

4.3.3 ETA for Hydrogen Accidents Sequences 74
4.4 Summary of the Safety Assessment Result 79
5 Safety Management of Hydrogen Accidents with SIS 81
5.1 LOPA for Hydrogen Accidents 81
5.2 SIS for Hydrogen Release 83
5.2.1 Sensor: Hydrogen Detector 85
5.2.2 Logic Solver: Safety PLC 87
5.2.3 Final Element 88
5.3 SIL Calculation for SIS 89
5.3.1 Safety Parameter for Components 89
5.3.2 Component PFD_G Calculation 90
5.4 Software Requirement 94
5.5 Summary of Safety Management of Hydrogen Accidents with SIS 96
6 Conclusions and Future works 97
6.1 Conclusions 97
6.2 Future Work 99
7 Bibliography 101
8 Appendix Numerical Solution for Equation 5.2 110

Abstract

The nuclear-based Cooper-Chloride (Cu-Cl) thermochemical cycle a promising method for future large-scale hydrogen generation. The nuclear-based hydrogen generation leads to new challenge for system safety due to the complexity of the co-generation system. In this research, a PSA-based framework for safety assessment and safety management of the nuclear-based hydrogen generation system is developed to perform a risk-informed design for Cu-Cl cycle. Two major safety challenges, LOCA and the hydrogen accidents, are analyzed in details with the PSA-based safety management framework. The PSA study shows that nuclear risks are effectively reduced by the reactor safety system, while the major risk is the hydrogen accidents. Based on the safety assessment result, safety instrumented system (SIS) is designed to control the hydrogen accidents. Different SIS configurations are compared numerically, which demonstrate the advantages of PSA-based methodology in controlling the uncertainty of the safety study.

Keywords: Nuclear-based Hydrogen Production, Probabilistic Safety Assessment (PSA), Safety Instrumented System (SIS), Fault Tree Analysis (FTA), Event Tree Analysis (ETA)

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my supervisor, Dr. Lixuan Lu, for giving me an opportunity to study in UOIT on this interesting topic. I would like to thanks for her invaluable guidance and continuous support for my Master research and study.

I would like to thank my thesis committee, Dr. Mikael Eklund, Dr. Dan Zhang and Dr. Atef Mohany, for their insightful comments and recommendations.

I want to thank my parents for their unconditional love and support for my study. Thanks for the support and encouragement during these years. I would not have been able to finish my program without their support.

In addition, I want to thank my uncle and my aunt for their continuous help during the last two years, as well as their valuable advices for finance, education and career.

Finally, I would like to acknowledge all the friends and faculty staffs in UOIT. Thanks for the wonderful campus life in UOIT.

List of Tables

Table 2.1 Safety goals result of Canadian commercial NPP 12

Table 2.2 Safety Integrity Levels.....15

Table 2.3 Reactions in the four-step Cu-Cl cycle.....20

Table 2.4 Thermochemical cycles for hydrogen production 22

Table 3.1 FTA symbols.....37

Table 4.1 Failure rate for heat exchanger primary loop.....64

Table 4.2 Failure rate for hydrogen generation 73

Table 4.3 Classification of flammable substances 75

Table 5.1 Severity levels and mitigated event target frequencies 83

Table 5.2 Comparison of hydrogen detection techniques 86

Table 5.3 Component failure rate 90

Table 5.4 Requirements for SRDT 95

List of Figures

Figure 1.1 Schematic of Nuclear-based hydrogen generation system 2

Figure 2.1 Process flow diagram of 4-step Cu-Cl cycle 21

Figure 3.1 Flowchart of PSA based safety management process 30

Figure 3.2 IPL for risk reduction 41

Figure 4.1 Heat transfer cycle for SCWR NPP 58

Figure 4.2 Intermediate heat exchanger 60

Figure 4.3 P&ID for heat exchanger 62

Figure 4.4 Fault tree for LOCA 63

Figure 4.5 Event tree for LOCA 66

Figure 4.6 Summary of LOCA outcomes 67

Figure 4.7 Hydrogen release CFD 69

Figure 4.8 Fault tree for hydrogen release 72

Figure 4.9 Event tree for hydrogen release 77

Figure 4.10 Summary of hydrogen release outcomes 78

Figure 4.11 Hydrogen accident distributions 79

Figure 5.1 SIS block diagram for hydrogen release 84

Figure 5.2 Ultrasonic leakage detector 88

Figure 5.3 SIS with redundancy.....91

List of Symbols

E: Input set for software

f: failure frequency

MTTR: Mean time to restoration (h)

P: Probability of failure

PFD_G: Average probability of failure on demand for the group of voted channels

T1: Proof test interval (h)

β : The fraction of undetected failures that have a common cause

β_D: The fraction of those failures that are detected by the diagnostic tests, the fraction that have a common cause

λ_D: Dangerous failure rate (per hour) of a channel in a subsystem, equal 0.5 λ

λ_{DD}: Detected dangerous failure rate (per hour) of a channel in a subsystem

λ_{DU}: Undetected dangerous failure rate (per hour) of a channel in a subsystem

List of Nomenclature

ADS: Automated depressure system

ALARP: As low as reasonably practicable

CCPS: Center of Chemical Process Safety

CDF: Core damage frequency

CERL: Clean Energy Research Laboratory

CFD: Computational fluid dynamics

CNSC: Canadian Nuclear Safety Commission

Cu-Cl: Cooper-Chloride

CVR: Coolant void reactivity

ETA: Event tree analysis

FMEA: Failure mode and effects analysis

FTA: Fault tree analysis

HAZOP: Hazard and operability study

IAEA: International Atomic Energy Agency

IEC: International Electrotechnical Commission

IPL: Independent protection layer

LBLOCA: large break loss of coolant

LCI: Low-pressure core injection

LOPA: Layer of protection analysis

LRF: Large release frequency

MPS: Passive moderator cooling system

NPP: Nuclear power plant

P&ID: Piping and instrumented diagram

PFD: Probability of failure on demand

PFH: Probability of dangerous failure per hour

PSA: Probabilistic safety assessment

PWR: Pressurized Water Reactor

RRF: Risk reduction factor

SBLOCAL: Small break loss of coolant accident

SCWR: Supercritical water reactor

SCW: Super Critical Water

SIF: Safety instrumented function

SIL: Safety integrity level

SIS: Safety instrumented systems

SRF: Small release frequency

SRDT: Software reliability demonstration testing

1 Introduction

This chapter presents the background, motivations, and objectives of the research for developing an integrated PSA-based framework for safety assessment and safety management of nuclear-based hydrogen generation with Cu-Cl cycle, as well as the organization of the thesis.

1.1 Background of Research

Hydrogen energy is a clean energy source that could provide a solution for the current energy problems such as global climate change, air pollution, and depleting fossil energy resources [1]. Hydrogen is the least polluting fuel of all natural or synthetic fuels. It is aboundant throughout the world. There are many methods to generate hydrogen, such as conversion of biomass and wastes, biological water splitting, photoelectrochemical water splitting, solar thermal water splitting and renewable electrolysis [2]. Nuclear-based hydrogen generation is one of the candidate solutions for large-scale hydrogen production in the future. Nuclear-based hydrogen production requires no fossil fuels, which results in lower greenhouse-gas emissions. The nuclear-based hydrogen production could lend itself to large-scale generation and has lower cost and higher efficiency compared with other methods.

Many nuclear-based hydrogen generation processes have been investigated in the world. One of these processes is the Cooper-Chloride (Cu-Cl) thermochemical cycle, which is developed by Canadian researchers. The schematic of nuclear-based hydrogen generation

plant is shown in Figure 1.1 [3]. The high energy-efficiency of 45% and low temperature-requirement makes Cu-Cl thermochemical cycle a promising method for future large scale generation of hydrogen energy [4, 5]. The Cu-Cl cycle is a set of closed loop chemical reactions for clean hydrogen generation from the thermochemical decomposition of water into hydrogen and oxygen. The intermediate copper and chloride compounds are recycled and reused within the thermochemical loop to continuously generate hydrogen without emitting pollutions and greenhouse gases.

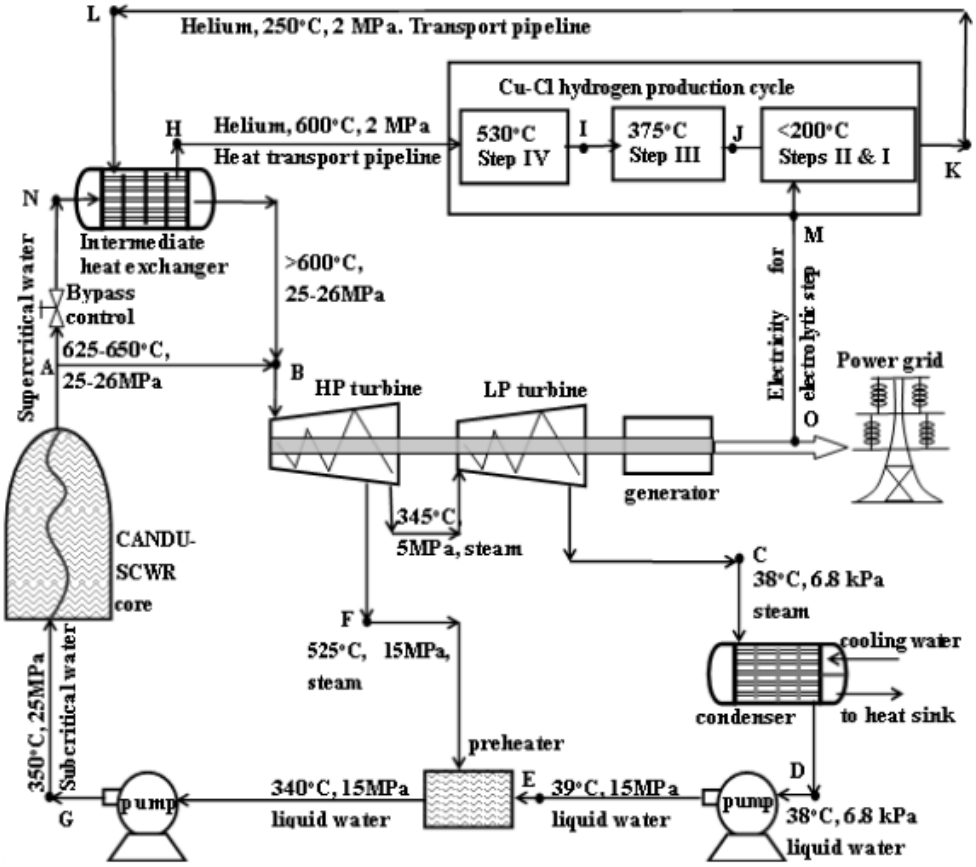


Figure 1.1 Schematic of Nuclear-based hydrogen generation system

The study of coupling the Cu-Cl cycle with a Generation IV Supercritical Water Reactor (SCWR), namely CANDU-SCWR, is carried out by UOIT and other organizations in Canada. The CANDU-SCWR uses super critical water (SCW) as the coolant for the nuclear reactor at pressure up to 25MPa and outlet temperature as high as 625˚C [6], which makes it possible to function as an energy source to power the Cu-Cl cycle.

However, the nuclear-based hydrogen generation leads to new challenge for system safety. On one hand, the hydrogen production facility is a new load for the nuclear reactor. The interconnection between a nuclear core and the Cu-Cl cycle is through a direct heat transfer loop. This new configuration carries external risks to the reactors through a direct heat-transferring loop interconnected with the reactor's coolant system. To avoid any potential severe nuclear accident due to malfunction of the hydrogen plant, the impact of hydrogen plant on the nuclear reactor safety should be carefully studied during all life cycle stages of the nuclear-based hydrogen generation project. On the other hand, the hydrogen production facility is a set of complex chemical processes, which inevitably exposes to internal process risks such as fires, explosions, releases of toxic or flammable chemicals. Project safety management to reduce the overall risks in the co-generation plant into an acceptable level should handle both the internal and external risks involved in the thermochemical water splitting process.

1.2 Motivation of Thesis

Safety management involves a set of principles, analysis, regulations and decisions to prevent injuries, death and property losses, which may be caused by potential risks within

a process or a system. It is essential to follow regulatory rules and criteria to build a hydrogen generation system with high level of safety. Probabilistic safety assessment (PSA) methodology has been used successfully in nuclear area and other fields as a powerful tool to assess safety and provide important information for decision-makings on design, development, operation, and maintenance of plants and facilities. In this thesis, a PSA-based safety management framework is developed to perform risk-informed design for the system safety of nuclear-based hydrogen generation and to control the potential risks within the hydrogen production process. The application of PSA methodology for safety assessment and safety management on the Cu-Cl cycle is presented to address the potential safety issues in a nuclear-based hydrogen production plant.

1.3 Objective of Thesis

The objective of the thesis is listed as below.

- Develop an integrated framework for safety assessment and safety management of nuclear-based hydrogen production based on the PSA methodology

- Application of PSA-based methodology to perform a preliminary safety assessment of nuclear-based hydrogen production plant to identify the major challenge for safety and the weakness of the current design

- Design and verification of safety instrumented systems (SIS) for risk prevention and mitigation in nuclear-based hydrogen production plant to control the potential risks

1.4 Organization of Thesis

The thesis is organized as follows: in chapter 1, the background, motivation, and objective for this thesis are provided. In chapter 2, a literature review is performed to investigate the most recent research findings in the fields of safety assessment and management of nuclear-based hydrogen production. The integrated framework for safety analysis and safety management based on PSA methodology is described in chapter 3. The following two chapters present the practical application of PSA-based methodology in the nuclear-based hydrogen production. The preliminary safety assessment processes and corresponding results are shown in chapter 4 and the design and verification of safety instrumented systems is represented in chapter 5. The conclusions and the recommendations for future works are given in chapter 6.

2 Literature review

This chapter reviews the previous findings related to the PSA of nuclear power plant (NPP), SIS, and safety studies of nuclear-based hydrogen production.

2.1 PSA in Nuclear Power Industry

2.1.1 Safety VS Reliability

Reliability and safety are both important features of systems. In safety engineering, they are different but related concepts, and sometimes been misused and abused. Reliability is the probability that an item will satisfactorily function over a period of time under given conditions. It refers to the occurrence frequency of a failure in a component or system. Safety is a combination of reliability, and the degree and consequences of failure. Safety represents the probability and ability of a system to keep freedom from the conditions that can cause injury, death, and loss of property or environmental damage under stated conditions in a specified period. In the safety engineering view, all failures challenge the reliability of a system. However, not all failures challenge the system safety. In other words, the set of failures for safety must be a subset of failures for reliability [7]. An example to illustrate the relation of safety and reliability is that many systems are designed to fail into a safe state. Even though some part of a system fails to function, the system does not perform any unsafe behavior.

2.1.2 Overview of PSA in Nuclear Power Industry

The PSA studies are not only a tool to quantitatively evaluate the risks in a system. They also provide important insights for safety management on design, operation, and maintenance of engineering systems. The first successful story of PSA application in nuclear power industry is the Reactor Safety Study WASH-1400 carried out for nuclear safety [8]. The objective of WASH-1400 is to numerically estimate individual and population accident risks from the operation of US commercial nuclear power plants. This study concluded that human factors have the most significant impact on the reactor accidents, and the small break loss of coolant accident (SBLOCA) is the major threatening initiating event for Pressurized Water Reactor (PWR). Four years after WASH-1400's first publication, this conclusion was proved by a severe nuclear meltdown accident in one of the two Three Mile Island nuclear reactors. Since then, PSA has been applied for safety study of many existing nuclear plants, and for the design and licensing of new plants in nuclear power industry. In addition, the PSA methodology has been adopted by many other industries including the process industry, transportation industry, space industry, where the system has safety critical functions.

PSA provides a systematic framework for safety analysis of nuclear power plant. It is a numerical evaluation method for assessing the risks and accident sequences in a nuclear power plant, which assists safety related decision-making process in all stages of the nuclear power plant life cycle. PSA follows a consistent and integrated approach to identifying risks and consequences, which could be caused by a wide range of events and

conditions. In real industrial engineering project, fault tree analysis (FTA) and event tree analysis (ETA) are most commonly used method in the PSA study for the system.

2.1.3 Three PSA Levels

In application of PSA on nuclear power industry, three levels PSA are internationally accepted by in the nuclear safety engineers all over the world. They are briefly summarized as follows:

2.1.3.1 PSA Level 1

The level 1 PSA in nuclear safety is the initial level of a PSA [9] for nuclear reactor. All PSA study of existing nuclear power plant or new nuclear plant design starts with a level 1 PSA. The level 1 PSA focuses on the assessment of causes and consequences for severe nuclear accidents in plant design and operation, which could cause core damage of the nuclear reactor. The Level 1 PSA task involves initiating events identification, system modeling, and accident sequence quantification. The level 1 PSA determines the frequency of nuclear core damage and the contributor of potential risks to the overall probability of this accident. Both the initiating events, system conditions and responses of safety systems in the accident sequences, such as shutdown system response, reactor cooling system reactions and human factors, are assessed numerically in this level of PSA. The level 1 PSA reveals the weakness of the NPP design and provides essential information for safety improvement to prevent the accident. The level 1 PSA also provide initiating information as input for next level of PSA.

2.1.3.2 PSA Level 2

Level 2 PSA starts with the result already undertaken in Level 1 PSA [10]. Level 2 PSA also addresses the issue of reactor's core damage accident, but mainly performs the post-accident assessment for the response of reactor containment and its related systems, such as the containment building and the containment cooling system. Level 2 PSA is integrated with the Level 1 results, to determinate the quantities and frequencies of radionuclides released to the environment after a core damage accident. The level 2 PSA provides a deeper insight into the strength and weakness of the nuclear containment integrity, which helps the improvement of containment safety design. The level 2 PSA provides information for improvements in prevention and mitigation of radionuclides releases in a severe core damage accident.

2.1.3.3 PSA Level 3

Started with the result undertaken in level 1 and level 2 PSA, the level 3 PSA [11] gives a full scope of the long-term distribution of radionuclides to the environment and the off-site risks to public health and environment due to postulated accidents. The level 3 PSA covers a broad range assessment in health and socioeconomic impacts leading from the post-accident release.

2.1.4 PSA in Canadian NPP

The national standards for nuclear PSA practice in Canada have been published by Canadian Nuclear Safety Commission (CNSC) as a regulatory framework for nuclear

safety of existing and new design of NPP in Canada. The important PSA-related standards in Canada are summarized below.

2.1.4.1 RD-337: Design of New Nuclear Power Plants

The standard RD-337: Design of New Nuclear Power Plants [12] figures out the design expectations of the new water-cooled NPP. RD-337 provides criteria for nuclear safety designs, as well as examples of possible optimization of design characteristics. RD-337 is built on the fundamental principles proposed by the International Atomic Energy Agency (IAEA) in NS-R-1: Safety of Nuclear Plants: Design [13]. Besides just fitting these principles into Canadian nuclear practices, the RD-337 goes beyond the scope of NS-R-1 by considering a broad range of interactions between NPP design and other issues, such as environmental protection, radiation protection, ageing and human factors. RD-337 gives three quantitative safety goals for Canadian NPP, and both the deterministic and probabilistic analysis methods to ensure these safety goals are discussed. The three quantitative safety goals for NPP in Canada are:

- Core damage frequency (CDF): "the sum of frequencies of all event consequences that can lead to significant core degradation is less than 10^{-5} per reactor year."

- Small release frequency (SRF): "the sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{15} Becquerel of iodine-131 is less than 10^{-5} per reactor year. A greater release may require temporary evacuation of the local population."

- Large release frequency (LRF): “the sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{14} Becquerel of cesium-137 is less than 10^{-6} per reactor year. A greater release may require long term relocation of the local population.”

2.1.4.2 S-294: Probabilistic Safety Assessment (PSA) for Nuclear Power Plants and Amendment

The standard S-294: Probabilistic Safety Assessment (PSA) for Nuclear Power Plants gives the fundamental regulatory requirement for PSA in Canadian NPP [14]. S-294 adopts the principle of three levels of PSA and requires a facility specific level 2 PSA to be performed for all NPPs designing or operating in Canada. Other regulatory rules specified by S-294 include: the requirement of updating the PSA models every three years or right after major changes in the facility, the requirement of model accuracy and assessment accuracy, the requirement of analysis coverage and the requirement of CNSC acceptance of methodologies and tools to be used for NPP PSA. An amended vision of S-294 has been issued in May 2014, namely REGDOC-2.4.2, Safety Analysis: Probabilistic Safety Assessment (PSA) for Nuclear Power Plants [15]. The amendment addresses the lessons learned from the Fukushima nuclear event of March 2011, and responses to the findings from the CNSC Fukushima Task Force Report [16].More details for probabilistic safety management requirements in Canadian NPP are given by the new vision. The major changes of REGDOC-2.4.2 from S-294 in PSA basis includes: an extension of model update interval from 3 years to 5 years and the additional assessment requirements for site-

specific initiating events and potential hazards, such as seismic hazards, external fires, external floods, high winds and severe weather conditions.

2.1.4.3 Safety goals result of Canadian commercial NPP

According the requirement of the nuclear safety standard, the PSA has been performed for the commercial NPPs. The safety goals achieved by some Canadian commercial NPP are represented in Table 2.1 [17].

Table 2.1 Safety goals result of Canadian commercial NPP

	Bruce A	Bruce B	Darling	Pick A	Pick B	Point Lepreau
SCDF*	3.0E-5	2.5E-5	7.9E-6	3.6E-5	4.2E-6	8.6E-6**
LRF*	8.9E-6	6.2E-8	5.2E-6	5.0E-8	3.9E-6	6.5E-8**

* Internal events **Post-refurbished state

Although nuclear safety has been extensively studied, there are limited studies regarding the linkage of nuclear power plant with chemical process. Since the PSA methodology has been proven to successfully address safety issues for nuclear power plant, the application of PSA-based safety regulation could be extended to use for the safety management of a nuclear-based hydrogen generation system.

2.2 Safety Instrumented System and Functional Safety

Safety combines both the reliability of a unit or system and the degree and consequences of failures. In safety management, one way to improve system safety is to increase the

inherent reliability of components in the system by using components that are more reliable, reducing the complexity of system structure or having some level of redundancy in critical components and subsystems. Another way to improve system safety is to reduce the frequency of occurrence for unsafe sequences of failures by providing additional protections and mitigations against failures to minimize the occurrence probability of accidental sequences into an acceptable level. Safety instrumented system (SIS) is a set of hardware and software components which works as independent protection layers between a critical process and its environment to minimize process risks for public as low as reasonably practicable (ALARP) by performing single or multiple safety instrumented functions (SIF). The safety instrumented system refers to a range of different applications and systems, such as safety shutdown systems, interlock systems, burner management systems and emergency shutdown systems.

2.2.1 IEC 61508 Standard

IEC 61508 [18] is an international standard issued by International Electrotechnical Commission (IEC) to regulate the application of SIS for functional safety. Functional safety is the part of overall system safety, which depends on a correct response of a system or equipment to its inputs. IEC 61508 specifies the requirements on all life cycle stages of a SIS, including system design, development and certification stages. IEC61508 is the generic functional safety standard that covers all kinds of industries. IEC 61508 gives a realistic view of risks and safety in a process:

- risks can never be reduced to zero

- safety must be planned in the beginning of a project
- and the non-tolerable risks should be reduced to the acceptable level

IEC 61508 is a generic standard, and several industry specified standards have been developed based on requirements of IEC 61508. IEC 61511 [19] provides requirements and recommendations in the functional safety of process industries. IEC 62061 [20] is written to address machinery-specific safety issues. IEC 61513 [21] specifies the application of IEC 61508 in the nuclear industry.

2.2.1.1 Safety Integrity Level

Safety Integrity Level (SIL) is the numerically scaled indicator for levels of risk reduction. IEC 61508 defines four SILs to represent the ability of risk reduction of a system, which associated with probability of failure on demand (PFD) for low demand systems and probability of dangerous failure per hour (PFH) for system working in a high demand mode. The SILs and demand modes required for different SIS are shown in Table 2.2, where a SIL 4 system has the highest risk reduction abilities and SIL 1 system has the lowest.

Table 2.2 Safety Integrity Levels

Safety Integrity Level	Probability of failure on demand, average (low demand mode)	Probability of dangerous failure per hour (high demand mode)	Risk Reduction Factor (RRF)
SIL 4	10^{-4} to 10^{-5}	10^{-8} to 10^{-9}	100000 to 10000
SIL 3	10^{-3} to 10^{-4}	10^{-7} to 10^{-8}	10000 to 1000
SIL 2	10^{-2} to 10^{-3}	10^{-6} to 10^{-7}	1000 to 100
SIL 1	10^{-1} to 10^{-2}	10^{-5} to 10^{-6}	100 to 10

2.2.1.2 IEC 61513 Standard

IEC 61503 is the interpretation of IEC 61508 in the nuclear sector. This standard specifies the framework of SIS design of computer-based systems and the application of functional safety in computer-based nuclear system. Unlike other IEC 61508 based standards, the concept of SIL is avoid to use in IEC 61513 to classify the risk reduction levels of SIS. Instead, three classes of the computer-based I&C system are defined to map the system into equivalent function categories, based on deterministic criteria and engineering judgment about degree and consequences of failures. While, Only Class 1 systems are allowed to use for the most safety intensive applications such as the protection systems and safety actuation systems. Moreover, the usage of class 2 and class 3 must be limited in non-critical application such as control systems and HMI systems. Although different conceptual basis of safety classification are used, the safety life cycle of SIS in nuclear domain compliance with the mainstream of IEC 61508.

2.2.2 SIL Assessment

Evaluation of SIL for SISs has been extensively studied as an important issue. IEC 61508 framework requires a quantitative determination of SIL for verification and certification of any SIS. The complex features of SISs mainly cause the difficulty for SIL evaluation. The complexity of SISs embodied in two aspects, the structural complexity and the operational complexity. For one thing, SIS is complex engineering system which consists of a set of hardware and software subsystems including actuators, controllers, sensors and software components, and involves levels of redundancies to achieve fault tolerance. The system safety models should represent all component faults and their effects to system reliability. Meanwhile, external events such as fire and human factor need to be considered in some cases. Complexity of system structures leads to complexity in system modeling and reliability calculation. For another thing, the operations and functions of SIS are complicated. All operating states of the SIS such as diagnosis, proof test, maintenance, and repair would have direct impact on the system safety availability. So far, various PSA based methods has been studied to handle the complexity in evaluating SIL.

To address this problem for SIL assessment, some studies are focused on development of the advanced system modeling methods to handle the complexity in system safety modeling. FTA based approach has been proposed to model time-dependent system behavior by introducing the distribution of periodically tested component in conventional FTA [22]. Markov models [23] [24] are used for SIL assessment as a solution for modeling the system dynamic of multistate systems. Fuzzy logic [25] is applied in system models to

handle the uncertainties in safety system performance. To reduce the complexity of the structural-oriented modeling process, an alternative approach has been proposed to build a system model by functional-oriented means [26]. Computer aided system modeling tools has been develop for automatically creation of Markov models for system reliability analysis [27].

Other researches are aimed at the safety assessment of hardware and software integrations in SISs. The difficulty in modeling hardware and software integration is due to the difference in the nature of failures. Hardware has a time-related failure rate due to the hardware wear out process. Failure occurs when some form of stress exceeds the associated strength of the product. While software is a collection of instructions, which enables a system to perform a specific task based on hardware platform, and it cannot work alone without hardware. Software failure mechanisms are different from hardware failures in that all software failures are caused by residual design defects.

In IEC 61508, the software reliability of safety instrumented systems is qualified according to the life cycle management in the software development and testing. Unlike the probabilistic assessment approach used in hardware SIL evaluation, the software SIL assessment follows a deterministic approach. The reason why quantitative assessment is not widely used for software reliability is because the lack of a good model to reflect the software reliability behavior. The software behavior in reliability and safety is very hard to model with mathematical models, especially in the safety critical tasks where extremely low or zero failure rates are allowed. However, a lot of effort has been made to seek for a numerical model for software reliability.

The most popular software reliability modeling method is the reliability growth model. This model is based on the assumption that reliably of software will increase after a bug is removed. To use growth model in the critical application, a hybrid approach for software reliability quantification has been proposed for the software used in nuclear safety systems [28]. The approach combines the software verification and mutation testing for quantitative software reliability evaluation with the reliability growth model. The possibility and limitations of using software is discussed in [29], problems such as the sensitivity of inherent failure number estimation and lack of failure data in critical software in revealed. To assess the effect of developer's skills and experience to the final reliability of software product, an advanced growth model has been proposed by considering the human factor when building the software model [30].

The reliability growth models used to estimate the software reliability require a failure history, while the software for safety system has a much higher reliability than general-purpose software that rarely or never fails during testing. To overcome this difficulty, another approach for software reliability modeling, namely the input domain based model or domain based model [31], could be used for safety critical software modeling. The input domain based models treat the software as a functional black box, in which failures are only caused by the fault related software inputs. Software reliability is estimated by evaluating the occurrence probability of fault related inputs in the completely input domain of software. The Bayesian networks have also been investigated to use in the reliability estimation of software-based system [32]. In a Bayesian networks, the evaluation of

software reliability is achieved by the Bayesian interference of the safety related parameters of the software system.

2.3 Safety Management in Nuclear-based Hydrogen Generation

Nowadays, about 97% of the hydrogen production is generated by reforming fossil fuels, such as coal and methane. Establishing low-cost methods of generating hydrogen in large-scale is a key challenge of future hydrogen utilization. A promising technology of large-scale hydrogen production is thermochemical cycle based hydrogen production.

2.3.1 Cooper-Chloride (Cu-Cl) Thermochemical Cycle

The Cooper-Chloride (Cu-Cl) cycle consists of a set of chemical reactions to form a closed internal loop cycle to generate hydrogen from the thermochemical decomposition of water into hydrogen and oxygen. The intermediate copper and chloride compounds are recycled and reused within the thermochemical loop to continuously generate hydrogen without emitting pollutions and greenhouse gases. There are different variations of Cu-Cl cycles based on the thermochemical water splitting: five-step reactions, four-step reactions, and three-step reactions [33]. But they all have the same overall reaction: $H_2O(g) \rightarrow H_2(g) + 1/2O_2(g)$.

This thesis is focused on the configuration of a four-step Cu-Cl cycle, which has been integrated and demonstrated for lab scale hydrogen production in the Clean Energy Research Laboratory (CERL) at the UOIT. The reactions involved in the four-step Cu-Cl

cycle are given in Table 2.3.The process flow diagram of 4-step Cu-Cl cycle is shown in Figure 2.1.

Table 2.3 Reactions in the four-step Cu-Cl cycle

Step	Reaction	Temperature(˚C)
1. Hydrogen production	$2CuCl(aq)+2HCl(aq) \rightarrow 2CuCl_2(aq)+H_2(g)$	<100 (electrolysis)
2. Drying	$CuCl_2(aq) \rightarrow CuCl_2(s)$	<100
3. Hydrolysis	$2CuCl_2(s)+H_2O(g) \rightarrow Cu_2OCl_2(s)+2HCl(g)$	400
4. Oxygen production	$Cu_2OCl_2(s) \rightarrow 2CuCl(l)+1/2O_2(g)$	500

The maximum temperature required for Cu-Cl cycle is 530˚C. One of the candidate nuclear reactors as the energy source for the Cu-Cl thermochemical cycle is the SuperCritical Water-cooled Nuclear Reactor (SCWR). The SCWR is a Generation IV nuclear reactor, which uses SuperCritical light Water (SCW) as the coolant at pressure up to 25MPa and temperature as high as 625˚C.

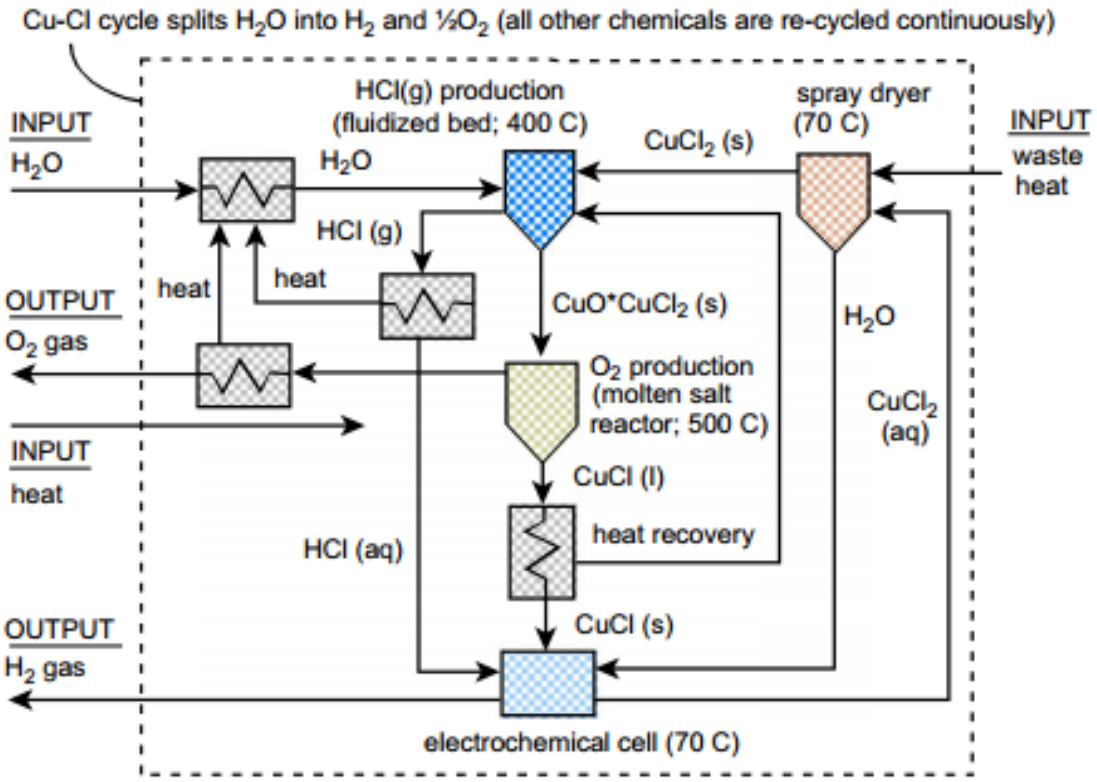


Figure 2.1 Process flow diagram of 4-step Cu-Cl cycle [34]

2.3.2 Other Thermochemical Cycles

Other Thermochemical cycles under development by other research organizations are listed in Table 2.4 as alternative solutions for nuclear-based hydrogen production [35]. As shown in Table 2.4, the major advantage of Cu-Cl cycle over other thermochemical cycles is the requirement of a relatively lower temperature.

Table 2.4 Thermochemical cycles for hydrogen production [35]

Cycles	Peak Temp (˚C)	Number of Reactions	Reported efficiency %
Sulfur-iodine	827-900	4	42-51
Hybrid sulfur	Not Given	3	41-53
Sulfur-bromine hybrid	Not Given	4	39
UT-3	750	4	40-50
Ca-Br-Star	750	3	44
Iron-chlorine	650	3	47-49
Copper –sulfur hybrid	827	5	86-73
Vanadium-chlorine	925	5	40.5-42.5

2.3.3 Summary of Safety Studies in Nuclear-Based Hydrogen Generation

Many researches on different thermochemical cycles for nuclear-based hydrogen generation have been carried out and most of these researches are focused on the area of thermochemical, thermal hydraulic, material, energy efficiency, and process simulation. The researches on the safety aspect of nuclear-based generation are limited, even though safety plays a very important role on both the nuclear side and the hydrogen side. This section will briefly review the existing works and achievements of safety studies in nuclear-based hydrogen generation system.

2.3.3.1 General safety analysis

The general safety issue for nuclear-based hydrogen production has been discussed in [36]. This study is not specific to any existing thermochemical cycle; however, it investigates the potential risks in worldwide nuclear-based hydrogen production activities and gives a generic overview of the potential safety challenges in future large scale hydrogen production. A comparison between the hydrogen and other conventional fuel gas is reported in this study, and current standards of the hydrogen safety are reviewed to point out the major safety concerns when using hydrogen in large scale as new energy.

Another report for the general safety issue comes from US researchers [37]. It is a study about the feasibility of nuclear-based hydrogen production with existing NPP. This report discussed the safety issues of nuclear hydrogen generation, as well as other topics such as

the economics, generation, storage, and transportation. The regulatory issues for hydrogen safety are the major safety concern of this study. It is reported that the existing standards and codes for hydrogen safety is mainly concerns about the hydrogen safety associated with fuel stations and hydrogen storage facilities, which deals with the safety in application of relatively small amount of hydrogen. As discussed in the report, no standard is available now to address the safety issue with large-scale production of hydrogen. It is highly recommended that such standard need to be develop to meet the requirements for future commercial scale hydrogen generation. Issues such as explosion, waste, toxicity, and location are also discussed in this work.

2.3.3.2 PSA in safety assessment of Hydrogen generation

Hydrogen related safety has been studied by PSA-based methods. A PSA study has been carried out to investigate the separation requirements for hydrogen plant and NPP [38]. A risk-informed separation distance has been calculated through a PSA model of hydrogen explosion caused by failures of the on-site hydrogen storage facilities. A reactor's core damage frequency due to hydrogen accidents has been reported as 7E-6 at the separation distance of 60m between hydrogen plant and NPP without additional mitigating features in between. The report also gives a comparison of core damage frequency with different separation distance and plants' configurations. Similar study has been carried out by [39] but through a semi-quantitative analysis approach. In both studies, it is assumed that a large amount of hydrogen gas is stored in the hydrogen plant. However, from the safety point of view, the on-site hydrogen storage quantity should be limited in the future design to reduce

the severity of hydrogen accident. Another available PSA is based on the conceptual design of hydrogen powered methane reforming process, which is theoretically not a thermochemical cycle [40]. An important finding from this paper is that in all the accidental outcomes, which could affect public health, the contributor of reactor core damage is very low, and the dominant risk in a nuclear-based hydrogen production process is the explosion of hydrogen, which contributes almost 90% to the total accident. The paper recommended the safety studies of nuclear-based hydrogen production should be concentrated on the hydrogen production plant.

2.3.3.3 Computational fluid dynamics in the safety study

Computational fluid dynamics (CFD) method has also been used in the safety assessment of hydrogen safety. Different from PSA based approach which models the probability and sequences of accident, the CFD study numerically simulates the accident scenario. A CFD based approach has been developed to determine the safety separation distance between nuclear plant and hydrogen facility [41].The CFD analysis models the overpressure of the hydrogen explosion, which is selected as the critical parameters by many hydrogen regulatory standards, to find a safe distance. In another application [42], the CFD method is used to perform a numerical simulation of the hydrogen and hydrogen chloride releasing from the Cu-Cl cycle. The flammable cloud formation process for hydrogen and the toxic cloud formation process for hydrogen chloride in a release scenario are modeled. In this model, only the release effect is considered, while the on-site storage of hydrogen is not included in this CFD study. The CFD calculation result shows that without bulky storage

of hydrogen in the plan, the pure hydrogen release accident could have minor impact on the nuclear power plant safety.

2.3.3.4 PSA in SIS used in thermochemical cycle

PSA has been demonstrated for designing and analyzing safety systems to mitigate the harmful sequence in accident associated with the nuclear-based hydrogen generation process [43]. In the previous researches, safety system is designed to stop or reduce the sequences of uncontrollable leakage of concentrated sulfuric acid in one reaction section of the S-I cycle. Multi-layers of protection systems are formed by three safety systems in the proposed solution. To optimize the proposed design, PSA is applied in reliability analysis of the safety structure to find the weakness part to be improved in the safety system.

2.4 Summary of Literature Review

PSA aims at evaluating the risks and accident sequences of a system. It has been standardized to use in nuclear industry and has been widely adopted by many other industries. Risks in a system can be reduced by active systems, which perform some function to mitigate or stop accident sequences. This kind of system is defined as SIS which plays a very important role in safety. IEC 61508 is an international standard about SIS, which requires a PSA to be used for quantitative determination of SIL.

Although safety is one of the major concerns in nuclear-based hydrogen generation, the safety features for the co-generation system has not been well studied yet. Previous safety

studies show the great potential of using PSA methodology to improve safety of nuclear-based hydrogen generation. To address the safety issues in nuclear-based hydrogen generation systems, an integrated framework of PSA-based safety assessment and management is developed in this thesis. Methodologies used in the PSA-based framework and the assessment result are presented in the rest part of this thesis.

3 PSA-based Safety Assessment and Management Framework

This chapter describes the methods and tools used in the safety management of nuclear-based hydrogen generation system. A PAS-based safety analysis and safety management framework is presented in this chapter. One of the greatest advantages of PSA-based methodology over other safety tools is the quantification of analysis results. The PSA results provide a more accurate insight of the safety features of systems, which are of great importance for decision-makings in design, development, optimization, validation, and certification of existing or new industrial systems. PSA could be used as a tool to assist safety management in all life cycle stages in a project. However, for project management, it is recommended that the safety should be considered as early as possible in a project design phase. The identification, control, and management of risks in early design stage of a project could efficiently reduce the unnecessary costs for system modification in later stages.

The Cu-Cl cycle is in its early development stage, where the studies in the aspects such as chemical, energy, material and economic of Cu-Cl cycle are currently based on the ongoing researches about the conceptual designs and the lab scale demonstrations. Due to the limitations, such as uncertainty for design specifics, lack of available data and potential changes in future stages, qualitative and semi-quantitative safety analysis tools are always been used in an early design stage. The application of PSA in the early design phase of Cu-Cl cycle has been demonstrated in this thesis. Our goal for the PSA study is to achieve

preliminary results of the plant safety and use these achievements in safety management to help improving the system safety.

This study focuses on the internal events in the nuclear-based hydrogen plant, while the external events such as floods, earthquakes, external fires, high winds, and thunders are not considered. In addition, this study aims at the short term and direct effects of accidents, such as system failures, release, fires, and explosions, during or after an accident. Long term accident scenarios such as long-term environmental effects and long-term public health effects, are not modeled and analyzed in this thesis.

3.1 Overview of PSA-Based Integrated Framework for Safety Management

A PSA-based integrated framework for safety management is developed in this thesis. The flowchart of the PSA based safety management framework is shown in Figure 3.1. The major tasks in the PSA based safety management are:

- A safety analysis and management process should be performed in the beginning of a new project or right after a critical change of design has been made. A safety study always starts with the identification of system to be analyzed. The main tasks in the system identification involve a study of system structure and system functions, defining system boundaries, collecting information from similar designs, and most importantly, make a decision whether a safety assessment is required and what level of details is expected from the safety study.

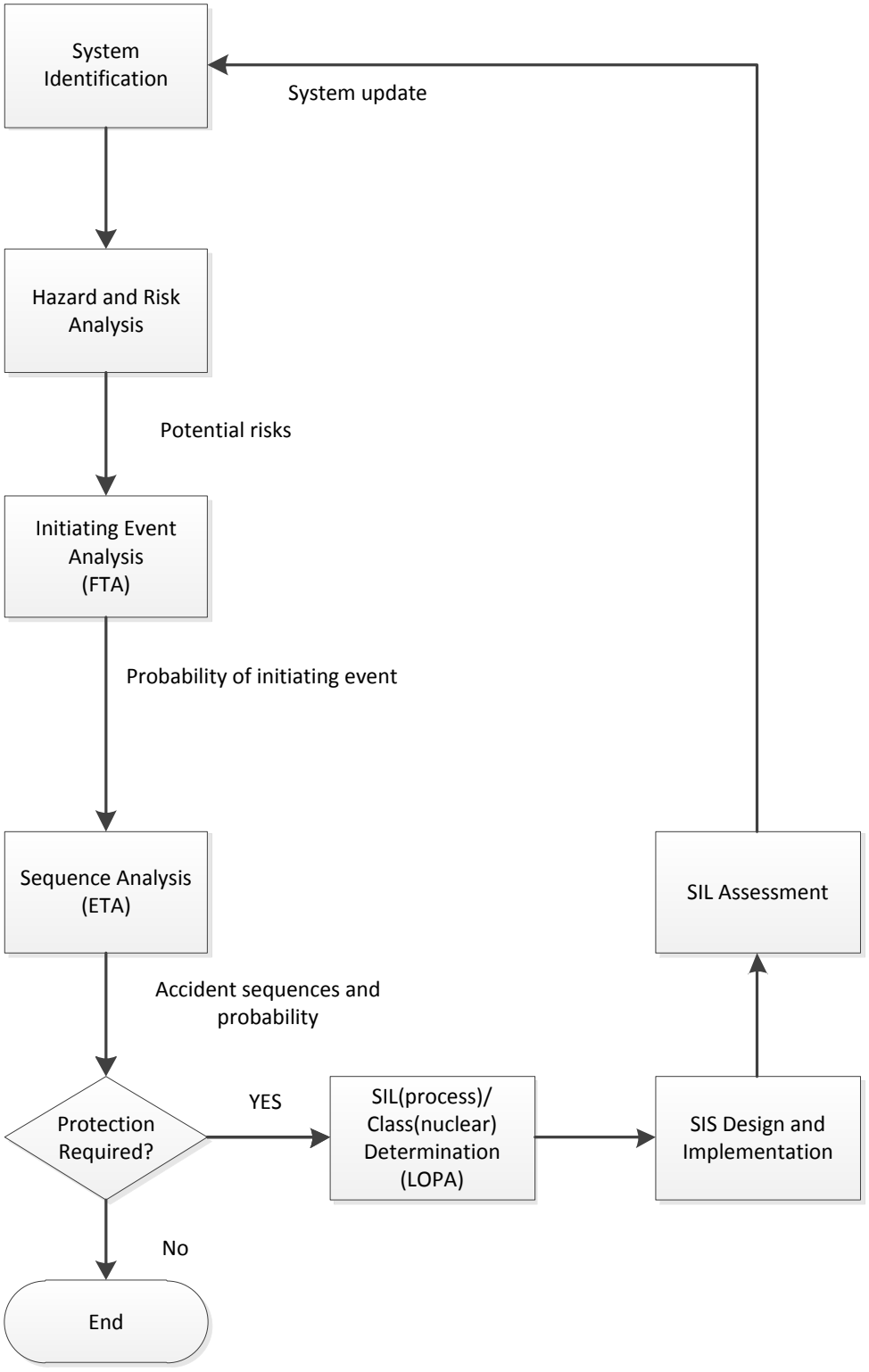


Figure 3.1 Flowchart of PSA based safety management process

- If a safety study is required to be made, the hazards and risks within the process should be analyzed to find the weakness and strength for the system. Based on the findings of the hazard and risk analysis, the initiating events for safety assessment are selected. The initiating events, which have potential risks to the system safety may be caused by a single failure or a combination of multiple faults and conditions within a system. To find the probability of causes of undesired events in the PSA-based framework, a FTA is performed to model the failure process of the system and calculate the probability of the accident occurrence as the top-event value in the FTA.

- The results of FTA would be used as the inputs for accident sequences analysis by the ETA. The purpose of ETA is to find all possible outcomes and their probabilities from an initiating accidental event. ETA considers more than just the inherent failures and risks in the system. More factors such as human behaviors, mitigation systems, environmental conditions, and emergency responses can be included in ETA when building the event tree. Besides the probability of occurrence for accident outcomes, the result of ETA also allows an investigation of the contributor of each accident to the total risks, the worst case scenario, the dominant risks, and the sensitivity of each sequence in an accident.

- A decision of whether additional safety protection layers are needed can be made upon the findings from ETA. This could be done by comparing the ETA results with the design basis or standards. In a safety view, all non-tolerable risks need to be reduced by safety systems. The level of risk tolerance can be determined with

the layer of protection analysis (LOPA). LOPA performs a semi-quantitative assessment to find the residual risks or non-tolerable risks in the system after all risk mitigation efforts have been carried out. As a result, it is determined in this step whether a SIS is required and if SIS is required to use, what risk reduction level should the SIS have to maintain enough safety.

- The international standard IEC 61508 standardizes the life cycle management of safety instrumented systems. The design and implementation of a SIS must follow the requirements and recommendations from IEC 61508, and all the design phases should be documented to prove the compliance of the standard. Technically, the risk reduction of a system or process could be achieved by reducing the occurring probability of the initiating events or by relieving the harmful risk sequences. A SIS always works as additional protection layers to prevent the occurrence of unsafe accident sequence. In addition, a quantitative SIL assessment must be carried out to ensure the required risk reduction level has been met with the SIS.

The rest part of this chapter will provide technical details about the methodologies used for safety study.

3.2 Hazard and Risk Identification

A safety life cycle always begins with the hazard and risk identification, follows by risk assessment, and finally finds solutions to control the risk. Hazard and risk identification plays an important role as initiating task for safety management. A correct understanding

of hazard and risk theory is critical. Although hazard and risk are always used interchangeable ways, there are essential differences between them.

- Hazard is defined as “an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment” [44]. Hazard is anything that can cause harm; it is the prerequisite for accident. Hazard is inadvertently built into systems, and it is a deterministic system property, not a random event.

- Risk is defined as “an expression of the impact and possibility of a mishap in terms of potential mishap severity and probability of occurrence” [44]. Risk is the chance that a hazard can actually do harm. Risk is a probability related concept; it is both the likelihood and severity of hazard outcomes. The risk can be defined by the formula:

$$\text{Risk} = \text{Probability} \times \text{Severity}$$

Hazard identification could be done by unbounded process or systematic and structured approach. The unbounded methods for hazard and risk identifications are performed with the expert judgment or brainstorm. The unbounded approach is easy to perform and it is good in identifying new hazard in novel designs. It is flexible to use in different types of systems. However, the accuracy and correctness of unbounded approach are heavily relied upon the skills and experiences of the examiner, which is the major disadvantage of this method.

Systematic hazard identification method is widely used in mature projects and many tools for systematic hazard and risk analysis have been developed:

- Hazard and operability study (HAZOP) is the most widely used hazard identification method and was developed by ICI in the late 1960s [45]. In HAZOP, the system is breaking down into subsystems based on the system function or structure. Critical parameters are selected and deviation guidewords are applied to each subsystem. The potential risks of these deviations is discussed and recorded. The system parameters could include anything the examiner may interest in: temperature, pressure, flow rate, level, speed, voltage, and current. Typical deviations might be: low, high, no, reverse, too low, too high, leakage, toxic, release, fire and explosion. A group of experts always conducts HAZOP and the parameters and guidewords need to be determined before the HAZOP. HAZOP can be used in a wide range of types of applications. The HAZOP will finally generate a detailed and auditable result. However, the HAZOP is usually time consuming and expensive and requires good preparation.

- Failure mode and effects analysis (FMEA) [46] is bottom-up deductive method for evaluating the effects of potential risks caused by failures in system. The purpose of FMEA is to identify failure modes of a system or subsystem, but it is also possible to perform FMEA in quantitative way by assigning the failure rate of each failure modes. A typical FMEA usually considers potential ways of failures, the possible causes, the failure effects, and mitigation and prevention methods.

- Hazard identification checklist is a list of known hazards or potential hazards. The listed hazards are derived from experience of risks assessment, history industrial data, or accident record for operation of similar systems. The hazard identification checklist should be prepared and authorized prior to use. Since potential risks are pre-listed, non-expert can use the checklist. However, disadvantage in using this approach is that the scope of analysis is limited by the risks listed in the checklist, so that it cannot reveal new hazard and risk, which are not pre-listed in the checklist.

3.3 Fault Tree Analysis

FTA was first introduced by the Watson of Bell Telephone Laboratories for the safety assessment in the project of control system of Minuteman missile launching in 1961. It has been wildly used as an important tool for probabilistic safety assessment.

3.3.1 Overview of FTA Methodology

FTA is a deductive approach for system safety modeling and analysis that could be evaluated qualitatively or quantitatively. The fundamental concept of FTA is to logically and graphically represent of combinations of faults, which lead to the undesired events associated with system. The FTA creates a bottom-up tree structure that maps all logic paths for initiating failures to the undesired fault. In quantitative assessment, Boolean logic is applied to all logic combinations of the faults to calculate the probabilistic value of the top event.

FTA is a systematic methodology for PSA. The theory behind the FTA is relatively simple and the application of FTA follows a straightforward approach, which make FTA suitable in modeling system failures for a wide range of industries. FTA provides a structured and layered approach to interpret combination of failures in a physical system into a logical diagram, which makes itself powerful to model a complex system.

3.3.2 FTA Symbols and Mathematical Basis

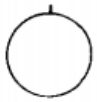
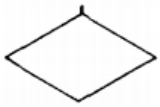
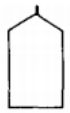
A FTA consists of the following steps:

- Top event definition
- Fault-tree construction
- Qualitative evaluation
- Quantitative evaluation

A fault tree is composed of a set of symbols for events and gates, the common symbols for FTA [47] are shown in Table 3.1.

To perform a quantitative evaluation with fault tree model, the probability is assigned for each basic event. The calculation process follows a bottom-up order to determine the probability of top events by applying Boolean logic to all combination of events through the logic gates.

Table 3.1 FTA symbols

Symbol	Description
	Basic initiating event that no further development is required.
	An undeveloped event, lack of information for event causes or consequence, or no need to develop.
	Conditional event or probability.
	Normal system condition, usually not a failure.
	AND Gate. The output occurs only when all input events occurs together.
	OR Gate. The output occurs if any input occurs.
	Exclusive OR Gate. The output occurs if only one input occurs.
	Priority AND Gate. The output occurs if the inputs occur in order.

3.4 Event Tree Analysis (ETA)

Unlike the deductive approach applied for FTA, ETA is an inductive method, which determines all possible outcomes and their probability of occurrence resulting from an initiating event. The system modeling process of ETA is different from FTA. In FTA, the cause and probability of a specific undesired event is modeled with all possible combinations of initiating events and conditions.

In contrast, the ETA is a top-down modeling process, which develops subsequent responses and their outcomes from a given initiating event. In system safety modeling, a combination of FTA and ETA is always used to develop a whole scope of system behavior in accident. Event tree models the system response and accident sequences, and fault tree evaluates the probability of different system behaviors in the case of an accident.

The ETA was first proposed and introduced in large-scale application by WASH-1400 [8]. In the WASH-1400 study, people realized the fault tree models for nuclear power plants growing too large to handle when several sequences are introduced into fault tree modeling. ETA is developed as an alternative method for FTA in modeling the outcomes from an accident.

A typical event tree usually has three components: initiating events, intermediate events, and end-state events. The initiating event is the root of event tree models. It is a state or condition of the system, which starts an undesired accident sequences. Intermediate events represent the possible responses of system following up with the initiating events. The

intermediate events are split into binary (yes/no) or mutually exclusive branches (multi-state), which means the events, which are represented by the branches, cannot occur at the same time. The end-state event is a condition of system when a harmful outcome is reached which cannot develop further or the point at which analysis of accident sequences is planned to stop. An ETA usually involves all or part of the following steps:

- System identification: define the system to analysis and system boundaries.
- Define the initiating events: system hazard and risk analysis to define possible initiating events.
- Define intermediate events: system response associated with initiating events.
- Build event tree: starting from initiating events until all end-states are reached.
- Obtaining probabilities for events: FTA can be used to calculate the probabilities.
- Quantitative assessment: determination of outcomes and their probabilities.
- Documentation: all analysis process should be documented and updated if new information is required.

The ETA represents the cause and effective of accident sequences in a visual way. It can be performed in different degrees of details. The major advantage of ETA for system safety modeling is its ability to model various responses from a wide range of subsystems including hardware, software, environment, emergency response, and human factors,

simultaneously for a complex engineering system to develop different accident scenarios.

.

3.5 Layer of Protection Analysis (LOPA)

The methodology of layers of protection analysis (LOPA) was first developed in 1990's when the SISs begins to become popular in safety management for different industries. The development of LOPA in history first started with the concept of layers of protection. The Center of Chemical Process Safety (CCPS) first proposed the concept of layers of protection and methods to determine the required number of layers in 1993. Later on, the procedures to perform LOPA were developed by some companies to solve practical problems. In addition, in 2001, a book was published by CCPS to describe the LOPA [48].

LOPA is typically a semi-quantitative safety assessment methodology that usually applied after a hazard and risk identification analysis to determine the required SIL for risk control and mitigation. The reason why LOPA is defined as semi-quantitative is because the numerical risk assessment is performed in the assessment approach and numbers as risk probabilities are used in the analysis. However, the numbers used for failure probability is usually selected to an order of magnitude level of accuracy. This would increase the uncertainty in the assessment result. To handle the uncertainty with assessment, an overestimating result is always expected to achieve from LOPA by taking the risks as large as possible, in order to consider the worst-case scenario.

To understand the theory behind LOPA, let us introduce the concept of independent protection layer (IPL) first. IPLs are systems, components, alarms, or actions against accidents, that when challenged by risks, designated functions are performed to preventing the accident sequences from reaching an unsafe end-state. The IPL requires each protection layer be completely independent of other protection layers, so the failures in one independent protection layer could not affect the functions in other layers. Each layers of protection has a safety integrated function (SIF) which is designed to avoid the occurrence of undesired events or mitigate the sequences from an initiating event. The risk reduction process with IPLs is shown in Figure 3.2, where the risk reduction factor of each IPL is associated with the layer's probability of failure on demand (PFD).

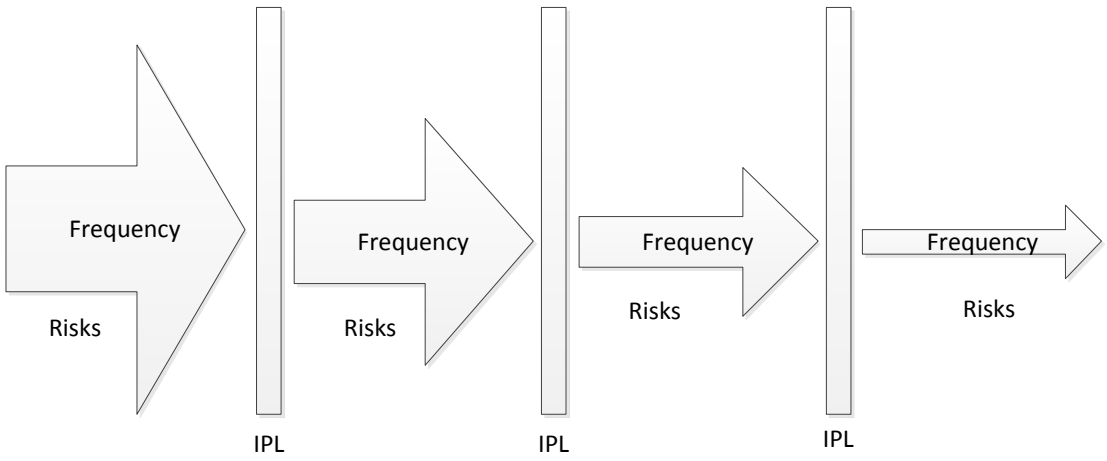


Figure 3.2 IPL for risk reduction

The modeling process and mathematical basis of LOPA and ETA are similar. However, the purpose of these two techniques in application is fundamentally different. ETA aims at

modeling all the causes and sequences of an accident. It considers all possible accident scenarios derives from an initiating event. It is a structured diagram representation of failures and effects in an existing system.

The LOPA is developed to evaluate the prevention and mitigation actions of a system and its protection layers against a specific accident. The role of LOPA in safety management is to investigate how risks are reduced within different protection layers and what is the effect of failures in protection layers.

If the LOPA indicates that the potential risks associated with a system or process cannot be tolerated with the current design. Then an effort must be made either to modify the design for more reliable structure or to reinforce the current design with additional protection layers. The risk reduction from design modification is always insufficient and costly in real industrial applications due to limitations of inherent features of system. Thus, in real application, a SIS is always designed as an additional protection layer. The design and implementation requirements are specified by IEC 61508 standard. As required by the standard a quantitative determination the SIL is of great importance in safety management of a project to ensure the overall safety reduction with the SIS. Because the correct functioning of SIS gives the last chance to bring the process back to a safe condition, in the worst case when all other designed protections are failed to work.

3.6 SIL Assessment

IEC 61508 uses the term of modes of operation to describe two types of safety functions implemented in SIS:

- The average probability of a dangerous failure on demand (low demand mode);
- The average frequency of a dangerous failure per hour (high demand or continuous mode).

Low demand mode is the SIS whose demand frequency of safety instrumented function (SIF) is less than once per year.

High demand or continuous mode is a SIS working condition where the demand frequency of SIF is more than once per year.

As a safety study on early design stage for nuclear-based hydrogen generation system, only the severe accident cases, which have most harmful consequences to the public, are considered in this thesis. The occurrence frequencies of severe accident are assumed lower than once per year, which will be proved in the analysis from following chapters. So, in this thesis, the SIL assessment for low demand mode is mainly discussed. The terms used to describe system reliability and safety, are listed in Table 3.2 [49].

- T1: Proof test interval (h)
- MTTR: Mean time to restoration (h)

- β : The fraction of undetected failures that have a common cause

- β_D: The fraction of those failures that are detected by the diagnostic tests, the fraction that have a common cause

- λ_D: Dangerous failure rate (per hour) of a channel in a subsystem, equal 0.5 λ (assumes 50 % dangerous failures and 50 % safe failures)

- λ_{DD}: Detected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)

- λ_{DU}: Undetected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)

- PFD_G: Average probability of failure on demand for the group of voted channels

- t_{CE}: Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all the components in the channel of the subsystem)

- t_{GE}: Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)

PFD average (PFDavg) is the average of probability of failure on demand, which is defined as:

$$PFDavg = \frac{1}{T}\int PFD(t)dt \tag{3.1}$$

3.6.1 Analytical Approach and Simplified Equations

Theoretically, SISs have a physical structure similar as other control systems, so most system reliability and safety modeling methods, such as Markov model, fault tree model, and reliability block diagram model, can be used for SIL assessment for SISs. In analytical evaluating approach, the SIL is derived directly from these system models of SIS. However, the complexity in system modeling and large amount of computations in system safety calculation makes the analytical approach inefficient to use in real project. To reduce the time and cost for SIL calculation, simplified equations are used alternatively to get an approximate evaluating result. The approximation result is able to meet the accuracy requirement in the analysis of industrial engineering systems. An example of simplified PFD calculation equation for a 1oo1 (1 out of 1) component is shown below:

$$\mathrm{PFD}_{\mathrm{G,\,lool}} = (\lambda_{DU} + \lambda_{DD}) \bullet t_{CE} = \lambda_D \bullet t_{CE} \tag{3.2}$$

Where:

$$t_{CE} = \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{3.3}$$

In the system level analysis, the PFD_G for an integrated system, which consist of sensors, logic solvers, and final elements, is calculated by adding the PFD_G value of different subsystems together.,

$$PFD_G = PFD_s + PFD_L + PFD_{FE} \tag{3.4}$$

The simplified equations are derived based on the approximation in the calculation of failure probability. It is assumed that the component used in SIS has a constant failure rate λ. The probability of failure occurs in this component or subsystem has an exponential distribution, which is:

$$P(\textit{failure}) = 1 - e^{-\lambda t} \tag{3.5}$$

Given a sufficiently small value x, the exponential e^x can be approximated as:

$$e^x \approx 1 + x \tag{3.6}$$

Rearrangement of the equation gives:

$$1 - e^x \approx -x \tag{3.7}$$

Substituting x with $-\lambda t$, yields:

$$P(\textit{failure}) = \lambda t \tag{3.8}$$

3.6.2 Software Reliability for SIS

Software plays a more and more important role in the SISs, because most control functions generated by the programmable logic controllers are software-based functions. The safety functions performed by the SIS require an interaction between hardware and software, in which the software processes the reading of the sensors and gives an output as the control signal to the equipment under control (EUC). The SIS will fail into a dangerous condition if the software has an incorrect response to the hazardous event when the SIS is expected to perform a safety function.

Unlike the hardware safety as discussed above, quantitative software safety assessment is not used in IEC 61508. Instead, the standard adopted a quality assurance approach for software safety, where the more stringent requirements put on the software the more reliable functions could be achieved. An input domain model based software testing approach is proposed in this thesis to address the problem of software safety in a quantitative way.

3.6.2.1 Input Domain Based Model

In the input domain based model [30], n inputs are randomly selected form the input data set $E=(E_i: i=1, 2, \dots, N)$, where E_i is the subset of software input domain. The inputs are sampled with the input distribution of operational profile $P=(P_i: i=1, 2, \dots, N)$; where P_i is the probability of choosing E_i as the input. If f failures are found in the execution of n inputs, then the software reliability can be estimated as:

$$R = 1 - f / n \tag{3.9}$$

When testing software with its input domain subsets, a prior knowledge of the system operational profile is required. The operational profile is a quantitative characterization of how the software is used in the real application. Musa [50] proposed a systematic approach to develop the operation profile for software testing. In the application of safety critical software test, the operational profile could be developed according to the operational history of plant or by expert knowledge. If the input distribution of the software is unknown, then the operational profile can be developed by assuming a uniform input distribution over the software input domain.

In a software and hardware integrated SIS, to have the SIS response successfully for a demand, the hardware should work in a failure-free condition and the software should process the output properly as designed and give a correct control command to hardware. Failures in either hardware or software could cause a failure on demand for the SIS. To represent in Boolean logic, the system will fail when "hardware fails" OR "software fails". Let us use the term PFD_{hw} to indicate the PFD for hardware subsystem and PFD_{sw} to indicate the PFD for software, where PFD_{hw} can be calculated from the equations given from IEC 61508 or analytical approaches, and the PFD_{sw} is the software reliability R determined with software testing. The PFD for system PFD_{sys} is expressed with the equation:

$$PFD_{sys} = PFD_{hw} \cup PFD_{sw} = PFD_{hw} + PFD_{sw} - PFD_{hw} \times PFD_{sw} \tag{3.10}$$

From the definition of PFD_G, the average PFD of system PFD_{sys} is the integral average of PFD_{sys}:

$$PFD_{sys,G} = \frac{1}{T_1}\int PFD_{sys,G}dt = \frac{1}{T}\int (PFD_{hw} + PFD_{sw} - PFD_{hw} \times PFD_{sw})dt \qquad (3.11)$$

As discussed above, the software reliability is time-independent, PFD_{sw} can be treated as a constant value when doing the integration, and thus the above equation is rearranged as:

$$PFD_{sys,G} = \frac{1}{T}\int PFD_{hw}dt + PFD_{sw} - PFD_{ws} \times \frac{1}{T}\int PFD_{hw}dt = PFD_{hw,G} + PFD_{SW} + PFD_{SW} \bullet PFD_{hw,G} \qquad (3.12)$$

Rearranging yields:

$$PFD_{SW} = \frac{PFD_{sys,G} - PFD_{hw,G}}{PFD_{hw,G} + 1} \qquad (3.13)$$

The SIS has a high reliability, so the $PFD_{,hw,G}$ is a small value . An approximation can be used to derive an simplified equation for practical application, for $PFD_{,hw,G} << 1$, $PFD_{,hw,G} + 1 \approx 1$. Thus, equation 3.13 can be rewritten as:

$$PFD_{SW} = PFD_{sys,G} - PFD_{hw,G} \qquad (3.14)$$

The average PFD for software (PFD_{SW}), is calculated from the system average PFD and the average PFD for hardware. This PFD_{SW} is used as the stop criteria for software testing. In a SIS which consist of a set of sensors, logic solvers and final elements, the $PFD_{hw,G}$ can

be derived with the simplified equation given by IEC 61508, and the $PFD_{SW,G}$ can be determined by substituting equation 3.4 into equation 3.14, which gives:

$$PFD_{SW} = PFD_{sys,G} - PFD_{hw,G} = PFD_{sys,G} - PFD_S - PFD_l - PFD_{FE} \qquad (3.15)$$

Where $PFD_{sys,G}$ is the PFD limit for given SILs, which is 10^{-1} for SIL1, 10^{-2} for SIL2, 10^{-3} for SIL3 and 10^{-4} for SIL4.

The software reliability PFD_{SW} is ensured by the software reliability demonstration testing (SRDT).

3.6.2.2 Software Reliability Demonstration Test

Numerically, if no fault is detected from the software test, then the reliability of software can be estimated as 1. However, a real software product will never get a 100% reliability unless the responses for all possible combinations of inputs are tested to be correct, which requires an infinite test. It is impossible to demonstrate software reliability with infinite test, due to the limitation of time and cost for testing. A decision must be made to stop the testing and put the system into operation. A Bayesian stopping rule [51] for safety critical software testing is proposed to calculate the minimal testing requirements for a stated SIL.

There are only two possible outcomes for each test case: fail or pass. If the SIS performs correctly when a safety function is on demand, then test is passed. While, if the system fails to response properly for a safety function demand, the test is failed. Assuming the value of probability of failure for software is p, where $PFD_{SW}=p$, the number of failures f from n tests follows a Binomial distribution:

$$P(F = f) = {}^{n}C_{f}\, p^{f} (1-p)^{n-f} \tag{3.16}$$

A prior conjugate is used to represent the changes of the parameter of interest p when extra information is collected from SRDT. The conjugate distribution of Binomial is the Beta(a,b) distribution:

$$f(p) = \frac{p^{a-1}(1-p)^{b-1}}{B(a,b)} \tag{3.17}$$

Where B(a,b) is the Beta function, a and b are parameters chosen by the assessor to represent the prior belief of the parameter p. If no prior information is available, a uniform prior could be used with a=b=1. If f failures are found from n tests, the posterior distribution of p is Beta (a+f,b+n-f):

$$f(p \mid f, n, a, b) = \frac{p^{a+f-1}(1-p)^{b+n-f-1}}{B(a+f, b+n-f)} \tag{3.18}$$

In the case of a uniform prior, the posterior distribution is:

$$f(p \mid f, n, 1, 1) = \frac{p^{f}(1-p)^{n-f}}{B(1+f, 1+n-f)} \tag{3.19}$$

Let the confidence level of the SRDT be C. The reliability requirement for a software test could be expressed as:

$$P(p < PFD_{sw}) \geq C \tag{3.20}$$

To meet the requirement for reliability PFD_{sw} and confidence C, the minimal successful executions without failure n_1 is the smallest value of n, which satisfies the equation:

$$\int_0^{PFD_{sw}} \frac{(1-p)^n dp}{B(1,1+n)} \geq C \tag{3.21}$$

If the failure occurs after s_1 ($s_1<n_1$) executions, the posterior distribution for p becomes:

$$f(p \mid 1, s_1, 1, 1) = \frac{p(1-p)^{s_1-1}}{B(2, s_1)} \tag{3.22}$$

It is also the new prior distribution for next software testing phase. The posterior distribution after n_2 failure free tests are observed is:

$$f(p \mid 1, s_1 + n_2, 1, 1) = \frac{p(1-p)^{s_1+n_2-1}}{B(2, s_1 + n_2)} \tag{3.23}$$

For a given requirement PFD_{sw} and C, the smallest value n_2 for failure free execution in the following stage of test after the fault is fixed could be solved from:

$$\int_0^{PFD_{sw}} \frac{p(1-p)^{s_1+n_2-1}}{B(2, s_1 + n_2)} dp \geq C \tag{3.24}$$

To continue this process, if the *j*th failure occurs on the s_jth test executions, the number of failure free execution for the next test stage (n_{j+1}) can be computed by solving the general equation:

$$\int_0^{PFD_{sw}} \frac{p^j (1-p)^{\sum_{i=1}^{j} s_i + n_{j+1} - j}}{B(j+1, \sum_{i=1}^{j} s_i + n_{j+1} - j + 1)} dp \geq C \tag{3.25}$$

A simplified stopping rule is developed to reduce the calculation for the process as described above. If j failures occurred, let the total number of executions until n_{j+1} failure free tests observed in the j+1th stage of test be N, where $N=s_1+s_2+\ldots+s_j+n_{j+1}$, which is the minimal number executions required to successfully demonstrated reliability with acceptable confidence level. Regardless of when these failures are happened during the test, this test process can be treated equivalently as a single test process in which j failures are observed out of N executions. To meet the requirement of software reliability, the total executions N that contains j failures should be the minimal value of N, which satisfies the equation:

$$\int_0^{F_{sw}} \frac{p^j (1-p)^{N-j}}{B(j+1, 1+N-j)} dp \geq C \tag{3.26}$$

According to the analysis above, the stopping rule for the software testing only depends on the total number of executions and the total number of failures out of these executions. Given a reliability requirement PFD_{sw} and C, the stopping rule for reliability test can be calculated before the test is carried out.

3.7 Summary of the PSA-based Framework

Safety must be considered as early as possible in an engineering project to avoid the loss of cost and time for design modification in late project stage. A PSA-based framework for safety assessment and safety management of nuclear-based hydrogen generation with Cu-Cl cycle is developed in this chapter. The purpose of the PSA-based methodology is to improve the system safety through an in-depth probabilistic model of system behaviors in the accident. The PSA-based framework identifies the occurrence probability of accident and models the accident sequences and their probabilities. In addition, other safety related system features, such as response of safety system, plant operating conditions, degree of fault, alarms and human factors, could be analyzed with PSA methodology. The PSA-based framework involves the safety modeling with FTA and ETA and the risk control with SIS. With the help of the PSA-based safety assessment, the designer could easily find the weakness part of the design through a systematic way and take actions to improve the system safety in the early design stage. The scope of the methodology is not limited to the safety study of Cu-Cl cycle. It can also be applied in the safety study for other engineering processes.

4 Safety Assessment Result

The safety assessment result for nuclear-based hydrogen production is represented in this chapter. The Cu-Cl cycle is still in its early design phase, no detailed design for Cu-Cl plant has been proposed so far. A preliminary safety assessment will be performed based on the currently available design phase information from public literature. The purpose of the preliminary assessment is to find the major hazard and risks in the Cu-Cl cycle, and assess their impact on the plant safety. As a conceptual design phase safety study, only severe accidents are considered. The safety assessment involves the hazard identification, fault tree modeling for initiating events, and event tree modeling for accident sequences. The numerical result is derived from the safety assessment, and this result is used to make a decision of whether additional safety management is required.

4.1 Risk and Hazard Identification

To start a PSA, hazard and risk in a process or system need to be identified first. Hazard and risk in a process or system can be identified with different methods as discussed before in chapter 3. The new safety issue caused by nuclear-based hydrogen production is the major concern for the safety research about the nuclear-based hydrogen generation with Cu-Cl cycle. To identify the new risk and hazard in a novel Cu-Cl cycle design, expert judgment for nuclear hydrogen production is referred.

According to the safety study proposed in previous literature [52], the following issues would be new risks in a nuclear-based hydrogen facility:

- Toxic chemical species: Hydrochloric (HCl) acid for the Cu-Cl cycle
- Hydrogen production and storage in large quantity: Hydrogen safety for production and storage
- Heat transfer fluids: additional thermo-hydraulic loop in the nuclear plant, LOCA must be analyzed

Although Hydrochloric acid is mentioned as a potential risk, it is not classified as major risk which could cause severe accident in the Cu-Cl cycle, in this thesis.

On one hand, the hydrochloric acid and hydrogen chloride has an irrigating and pungent odor even at very low concentration. It is very easy to detect when the HCl released into the environment. So, it is assumed in this thesis that the operator can detect and stop a leakage of HCl in early stage release by shutting down the process reactions.

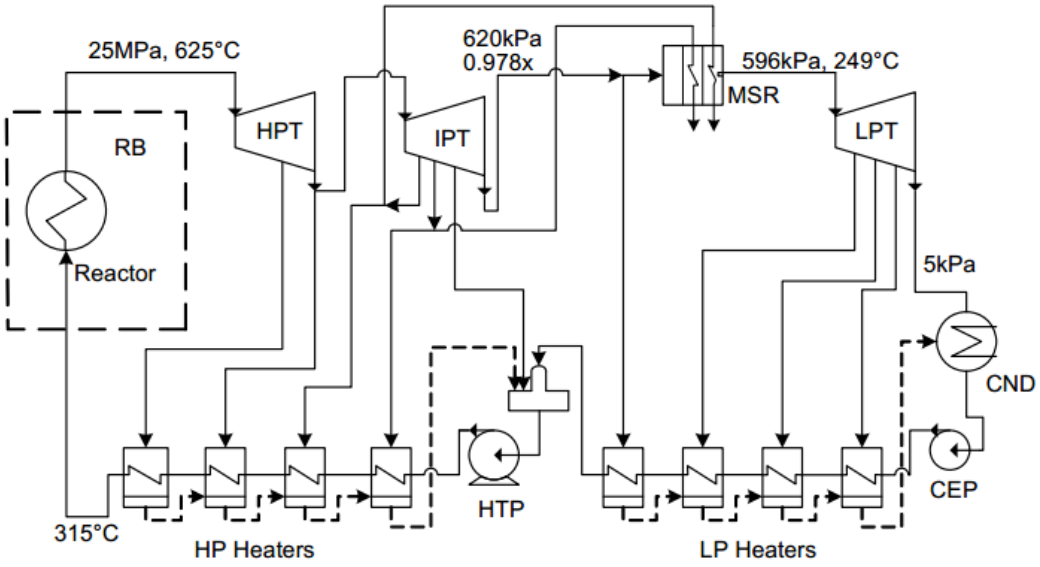
On the other hand, as an intermediate reactant, HCl recycles in the Cu-Cl thermochemical process, where it is generated and assumed within the reactions, as the process discussed in chapter 2. Although the total amount of HCl required for daily hydrogen production is very large, the actual amount of HCl exists in Cu-Cl cycle is small at one time. Therefore, the release of HCl could have minor effect, given a limited existing quantity in the Cu-Cl cycle.

Thus, in this thesis, the LOCA from the heat transfer loop and the hydrogen accident caused by undesired leakage are selected as the major risks introduced by Cu-Cl cycle, which will be studied by PSA-based approach in this chapter.

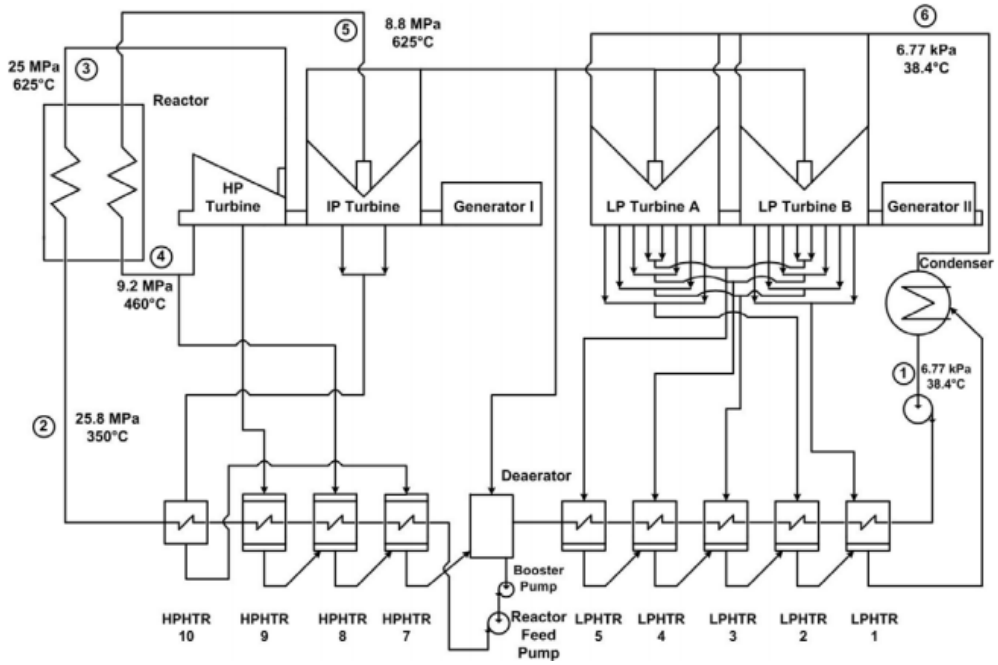
4.2 PSA for LOCA

In a Cu-Cl thermochemical hydrogen production plant, power from NPP is supplied to the thermochemical reactions as energy source for water decomposition. The CANDU-SCWR design has a once through direct coolant loop, where no intermediate steam generator is used as the heat transfer interface between the reactor core and the load. Different NPP heat transfer system has been proposed, for example, Figure 4.1 shows the layout of a no-reheating loop and single-reheat loop [53]. In general, the more heating loops a reactor have the higher energy efficiency could be achieved. However, the more heating loops will increase the system complexity and cost, so it is important to find an optimum layout for the cost and efficiency.

Loss of coolant accident is the accident when coolant releases from reactor's coolant system. In LOCA the nuclear reactor will loss part or total cooling ability, which is crucial to keep the reactor core in stable temperature and pressure. LOCA is the possible cause of some severe nuclear accident such as reactor core damage. The cause and effect of coolant release must be studied carefully to ensure a safer design for nuclear reactor. The result of PSA study for LOCA sequences is represented in this section.



(a) No-reheat Layout

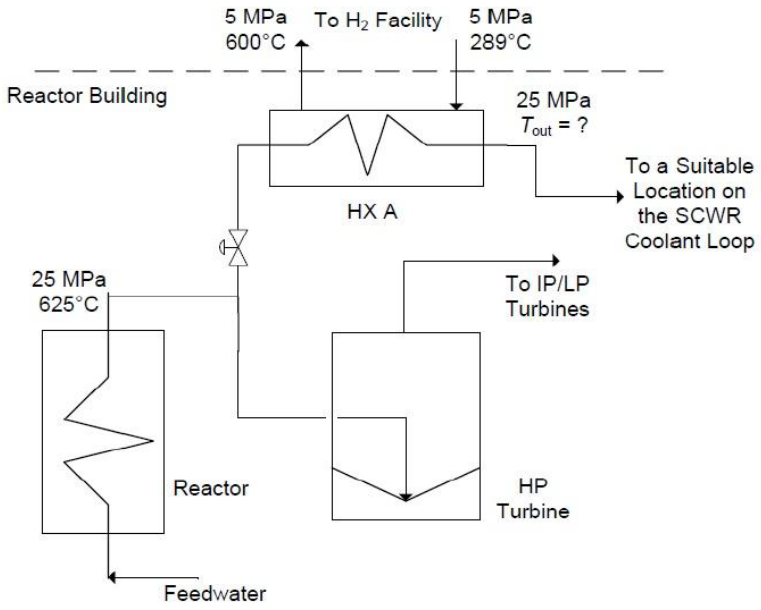


(b) Single-reheat Layout

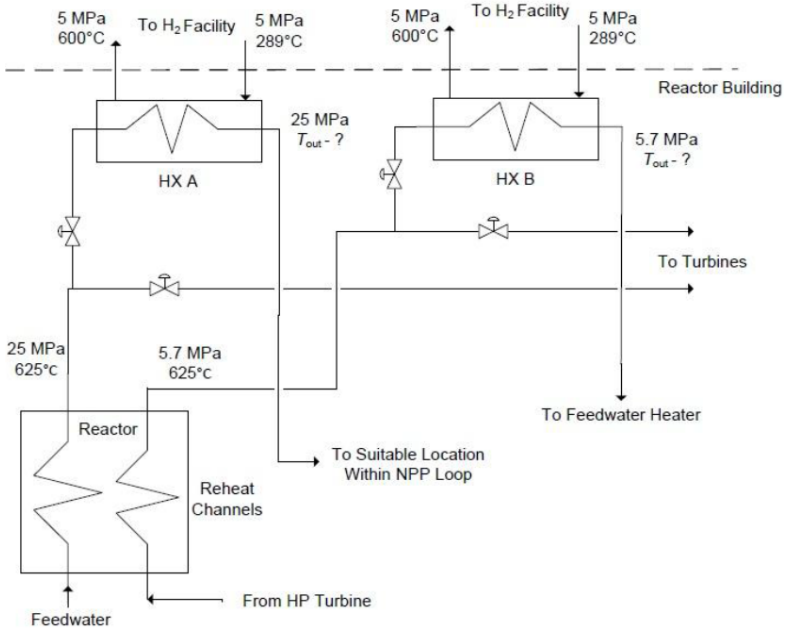
Figure 4.1 Heat transfer cycle for SCWR NPP [53]

4.2.1 Heat Exchanger System

A double pipe intermediate heat exchanger or a tube and shell heat exchanger can be used as an interface for transferring thermal energy from the reactor coolant system to the hydrogen production plant. The heat exchanger would be interfaced with the no-reheat alignment of coolant cycle or the single reheat alignment of the coolant cycle [54], as shown in Figure 4.2. In both linkage options, a location on the coolant loop downstream of the reactor and upstream of the turbine would be a suitable location for the heat exchanger. In this case, SCW is the operating fluid on the primary loop of heat exchanger.Also, for the single reheat cycle, a second available location would be downstream of the steam reheat channels and the operating fluid is the superheated steam. In both linkages, the reactor coolant is bypassed to the heat exchanger to power the hydrogen production and mixed back with the reactor coolant main stream. Although the heat exchanger thermal hydraulic behavior could be different between these two linkage options due to the operating fluid property diverse, the safety performance of these two systems can be similar, since both systems share the same control and instrumentation structures. Also it is assumed only one heat exchanger is functioning at a given time to transfer heat to hydrogn facility [54].



(a) Intermediate heat exchanger for No-reheat layout



(b) Intermediate heat exchanger for single-reheat layout

Figure 4.2 Intermediate heat exchanger [54]

4.2.2 FTA for LOCA

According to the available information about the heat transfer loop for hydrogen generation, the piping and instrumented diagram (P&ID) of the heat exchanger is shown in Figure 4.3. For plant balance, the amount of coolant deliverd to hydrogen plant is determined based on the electrical and hydrogen generation demand, which is contoled by an control valve located at downstream of reactor core. Here, it is assumed that the basic process control system is applied to control the heat exchanger, and no extra safety system is used. The heat exhanger loop consists of:

- Two isolation valves: isolate the heat exchanger from NPP coolant system
- Pipes
- Control valve: control the flow rate of heat exchanger primary loop
- Intermediate heat exchanger: double pipe or tube and shell
- Mix valve: mix the operating fluid from downstream of heat exchanger with NPP coolant main stream

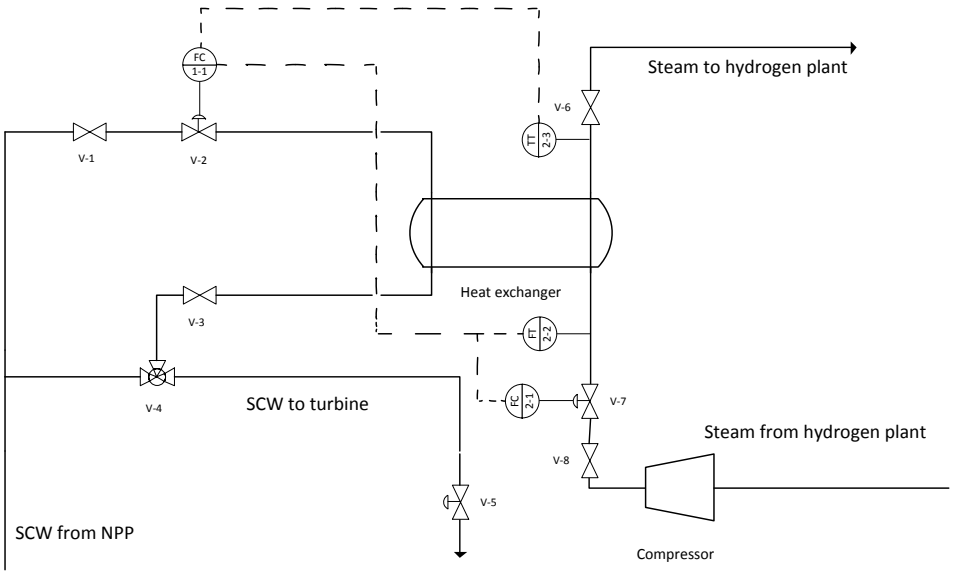


Figure 4.3 P&ID for heat exchanger

The LOCA is caused by any leakage in the heat transfer interface piping system. To identify the imitating event frequency of a LOCA due to hydrogen production, a fault tree is developed to calculate the LOCA probability as a top event. The fault tree is shown in Figure 4.4. The failure rate of basic events probability is shown in Table 4.1. In particular, the pipe failure rate is related to the length of the pipe. According to the current Cu-Cl design specifications, the heat exchanger is located in the nuclear containment building. Thus, it is assumed the pipe length of heat exchanger primary loop is in the range of 100 meters. In this analysis, the value for pipe length is taken as 100 meter.

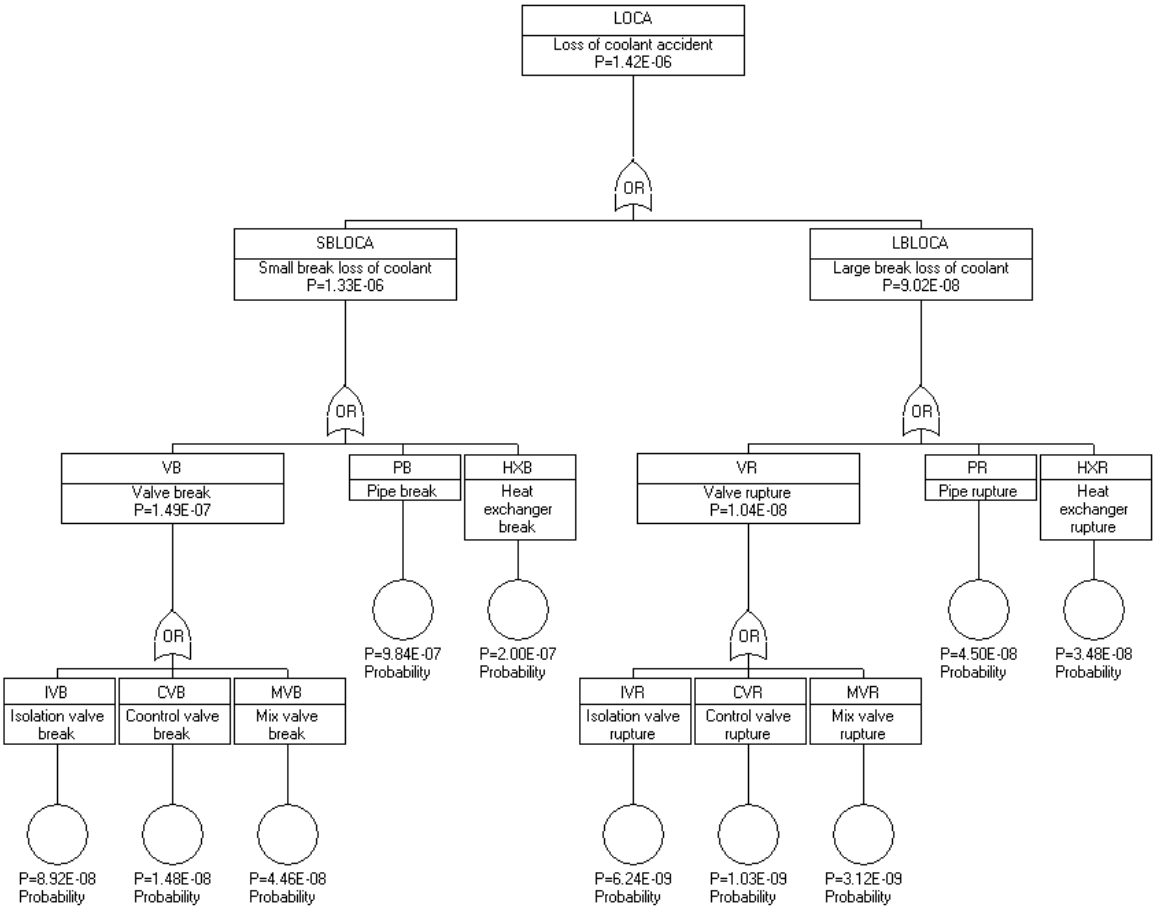


Figure 4.4 Fault tree for LOCA

Table 4.1 Failure rate for heat exchanger primary loop

Code	Description	Available Source*	Selected value	Comment
IVB	Isolation valve break	NUREG: 4.46E-8/h E&R: 1.0E-8/h	8.92E-08/h	Two isolation valves in loop
CVB	Control valve break	NUREG: 1.48E-8/h E&R: 1.0E-8/h	1.48E-08/h	
MVB	Mix valve break	NUREG: 4.46E-8/h E&R: 1.0E-8/h	4.46E-08/h	
PB	Pipe break	NUREG: 6.89E-10/h-ft E&R: 3.0E-9/h-ft	9.84E-7/h	100m
HXB	Heat exchanger break	NUREG: 2.0E-7/h E&R: 1.0E-7/h	2.0E-7/h	Tube leakage
IVR	Isolation valve rupture	NUREG: 3.12E-9/h E&R: 1.0E-10/h	6.24E-9/h	Two isolation valves in loop
CVR	Control valve rupture	NUREG: 1.03E-9/h E&R: 1.0E-10/h	1.03E-9/h	
MVR	Mix valve rupture	NUREG: 3.12E-9/h E&R: 1.0E-10/h	3.12E-9/h	
PR	Pipe rupture	NUREG: 1.38E-10/h-ft E&R: 3.0E-11/h	4.5E-8/h	100m
HXR	Heat exchanger rupture	NUREG: 3.48E-08/h E&R: 1.0E-9/h	3.48E-08/h	Tube Rupture

* *NUREG* [55]*: NUREG/CR-6928 Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.*

E&R [56]*: Component external leakage and rupture frequency estimates.*

The LOCA can be classified as small break loss of coolant accident (SBLOCA) and large break loss of coolant (LBLOCA) depending on the leakage size in the coolant system. Based on the FTA, the SBLOCA due to hydrogen production is 1.33E-6/h and the LBLOCA frequency is 9.02E-8/h. The original value is multiplied by 8760 to convert into the frequency of each year (1year=8760h), which is 1.17E-2/y for SBLOCA and 7.9E-4/y for LBLOCA. The result is in the same range of LOCA value in other CANDU NPP [57]. In this study, the SBLOCA and LBLOCA are combined together as an overall LOCA event, because the SCWR safety system performance is similar in both scenarios [58]. The total occurrence frequency of LOCA is 1.27E-2/y.

4.2.3 ETA for LOCA

The response of reactor safety system in the event of LOCA is analyzed as the accident sequences with the event tree model. The event tree analysis of CANDU-SCWR is based on the safety study of CANDU-SCWR described in [58]; the event tree is shown in Fig 4.5.

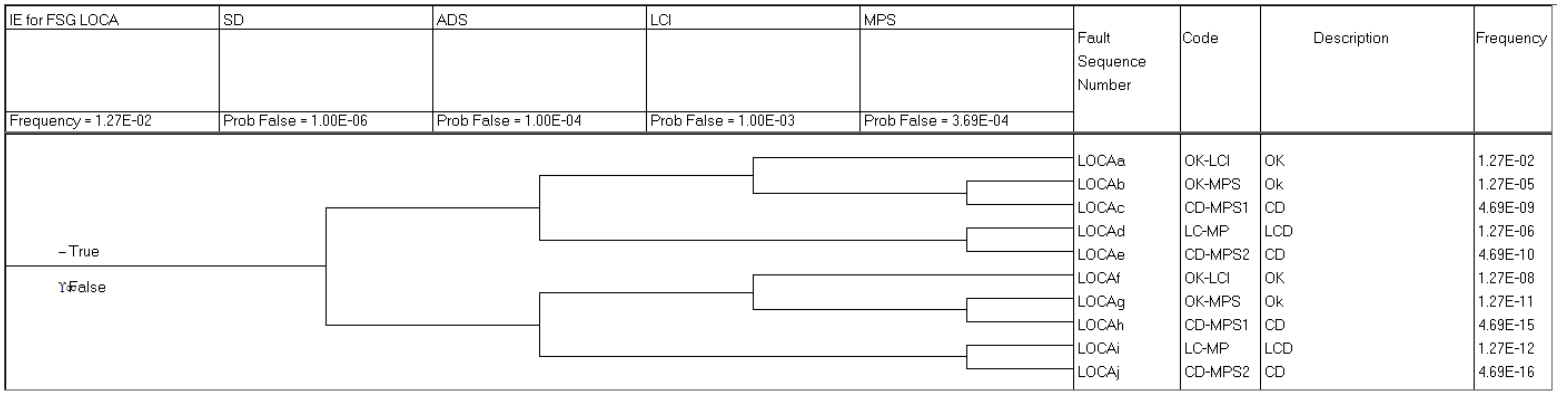


Figure 4.5 Event tree for LOCA

Compared with existing Candu reactors which have a positive coolant void reactivity (CVR), the CANDU-SCWR has a negative reactivity on coolant voiding which will slow and eventually stop the fusion process in a LOCA. Similar as the other CANDU reactor, two independent shutdown systems will activate to ensure a minimal loss of inventory prior to trip. The residual heat generated from the LOCA is removed by the Emergency cooling system which consists of pumped or gravity-fed automated depressure system (ADS) and low-pressure core injection (LCI). An ADS is capable of sustaining blowdown cooling for a period of some 10s of seconds for rapid depressurization, and the LCI supplies water to the reactor core during emergency cooling conditions. If all the safety system failed, the use of a passive moderator cooling system (MPS) is the last line of defense to keep the core cool in the case when cooling capability is lost. The summary of LOCA outcomes is shown in Figure 4.6

Outcome Code	Outcome Description	Outcome Frequency
CD-MPS1	CD	4.69E-09
CD-MPS2	CD	4.69E-10
LC-MP	LCD	1.27E-06
OK-LCI	OK	1.27E-02
OK-MPS	Ok	1.27E-05

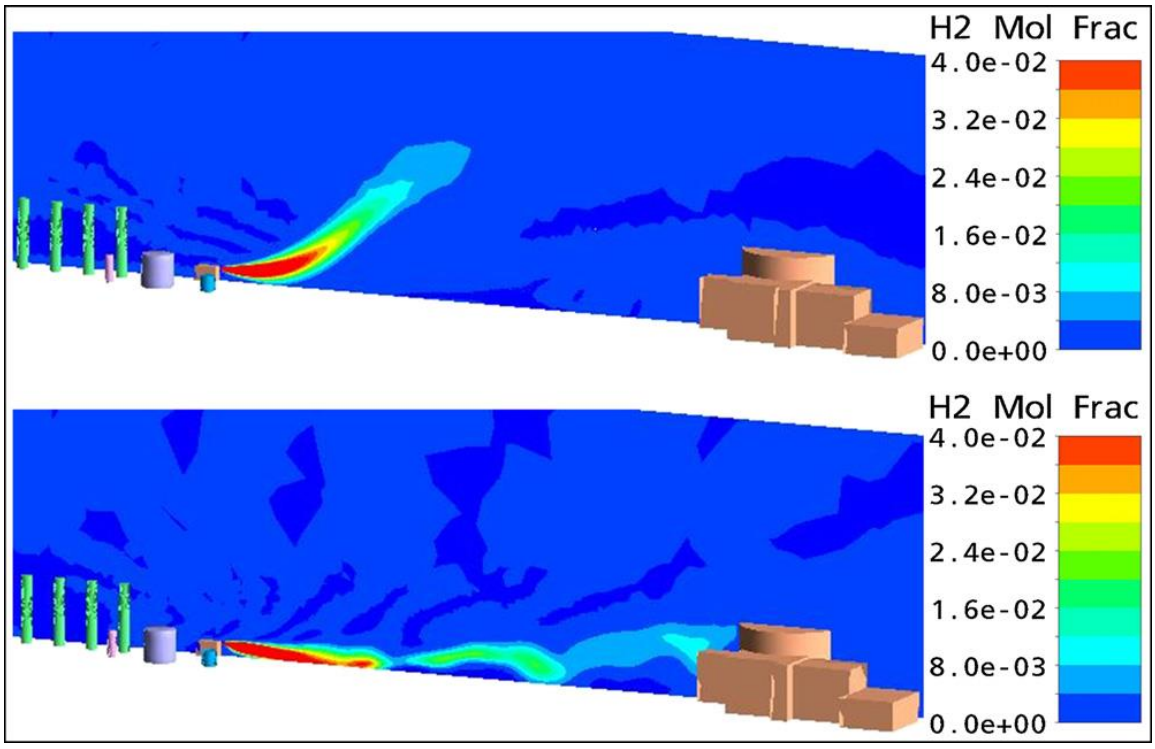
Figure 4.6 Summary of LOCA outcomes

In Figure 4.5 the state OK-LCI implies the reactor core successfully gets long-term cooling from the LCI after the reactor shutdown. In the situation when the LCI fails and MPS works, the core can still be kept cool (OK-MPS). In the situation where ADS fails and MPS works,

limited core damage is caused due to the delay in core cooling from MPS (LC-MP). Core damage occurs when the MPS fails together with either the ADS or the LCI (CD-MPS1 CD-MPS2). In summary, the severe core damage probability due to the interfacing with hydrogen production is 5.1e-9/y. This value is significantly lower than the safety target of the nuclear design basis failure frequency. This PSA result implies that the additional risks for nuclear safety caused by the linkage with hydrogen plant can be effectively eliminated by the nuclear safety system. So, no extra safety system is required to control risks from heat interface between NPP and hydrogen plant.

4.3 PSA for Hydrogen Accidents

The hydrogen accidents such as fire and explosion are possible to cause a nuclear safety related accident if the blast wave of hydrogen explosion carries enough energy that destroys the safety barriers of the NPP. However, the impact of the hydrogen accident on the NPP highly depends on the amount of hydrogen storage inside the generation plant and the separation distance between NPP and hydrogen plant. The hydrogen release in the Cu-Cl process has been modeled with CFD [42] and the flammable hydrogen cloud distribution is shown in Figure 4.7. The mass of flammable cloud is between 1.76kg and 1.78kg, and the volume is about 400 m^3. An explosion experiment with similar amount of hydrogen shows that the blast wave is 10kPa at about 62m form the edge of cloud, which cannot produce serious structural damage for NPP. The CFD analysis draws the conclusion that at a separation distance of 100m the explosion caused by hydrogen leakage to the open atmosphere has limited effect to the NPP.



Hydrogen molar fraction after 500s of release from the high pressure pipe with 1 m/s wind (Top) and with 10 m/s wind (Bottom). The wind direction is from left to right. The red colour identifies the hydrogen cloud with a volumetric concentration equal or larger than 4%.

Figure 4.7 Hydrogen release CFD [41]

Because the layout of the nuclear-based hydrogen plant is still not finalized now in the design phase, it is hard to estimate how much hydrogen gas would be stored in the hydrogen facility and what is the final separation distance between two plants from existing research results. However, in accordance with the inherently safer design philosophy [59], the risks in the process could be reduced or eliminated by minimizing the quantities of hazardous material. So, it is assumed in this thesis that the future design of hydrogen plant will

significantly reduce the amount of hydrogen appears in the hydrogen plant to achieve a better inherent safety, by immediately deliver the hydrogen gas to the hydrogen storage facility settled at a safety distance from both the hydrogen plant and the NPP. Based on this assumption, the amount of hydrogen involved in a hydrogen accident is limited by the generating rate of hydrogen. Only the release from continuous hydrogen generation is analyzed. So the boundary for PSA of hydrogen accidents is limited within the hydrogen facility.

4.3.1 Hydrogen Accidents Overview

Hydrogen is a flammable, colorless, tasteless and odorless gas. As a hazardous resource in the process industry, hydrogen has unique properties, such as ease of leaking, wide range of combustible mixture and low-energy ignition. The production, distribution and use of hydrogen as a primary energy source pose new safety challenges.

Hydrogen is generated with the CuCl/HCl electrolysis reaction. The main equipment used for hydrogen generation is the electrolyser, in which the hydrogen gas is produced at the cathode. The lab scale hydrogen production with electrolyser has been demonstrated at AECL [60]. In future large scale hydrogen production system, the industrial electrolyser will consist of a bunch of individual electrolysis cells. The reactant is delivered into each reaction cell evenly, and the hydrogen is generated at the cell's cathode. hydrogen gas is collected from the cells through pipes inside of the electrolyser and delivered together to storage and distribution facilities. As mentioned before, the hydrogen storage and distribution facilities are located at a safety distance away from both the hydrogen plant

and the NPP. It is assumed that the basic control system is applied to keep a continuous reaction in electrolyser.

4.3.2 FTA for Hydrogen Accidents

The initiating event for a hydrogen accident is the release of hydrogen gas from the hydrogen production reactor. Hydrogen would release from any leakage of piping and equipment, or from the loss of containment of the electrolyser due to the reactor overpressure. Figure 4.8 shows the fault tree for the hydrogen release. The failure rate of basic events is shown in table 4.2. The pipe length is assumed in the range of several 10s of meters to 100 meters, because a hydrogen explosion will have minor effect beyond that range.

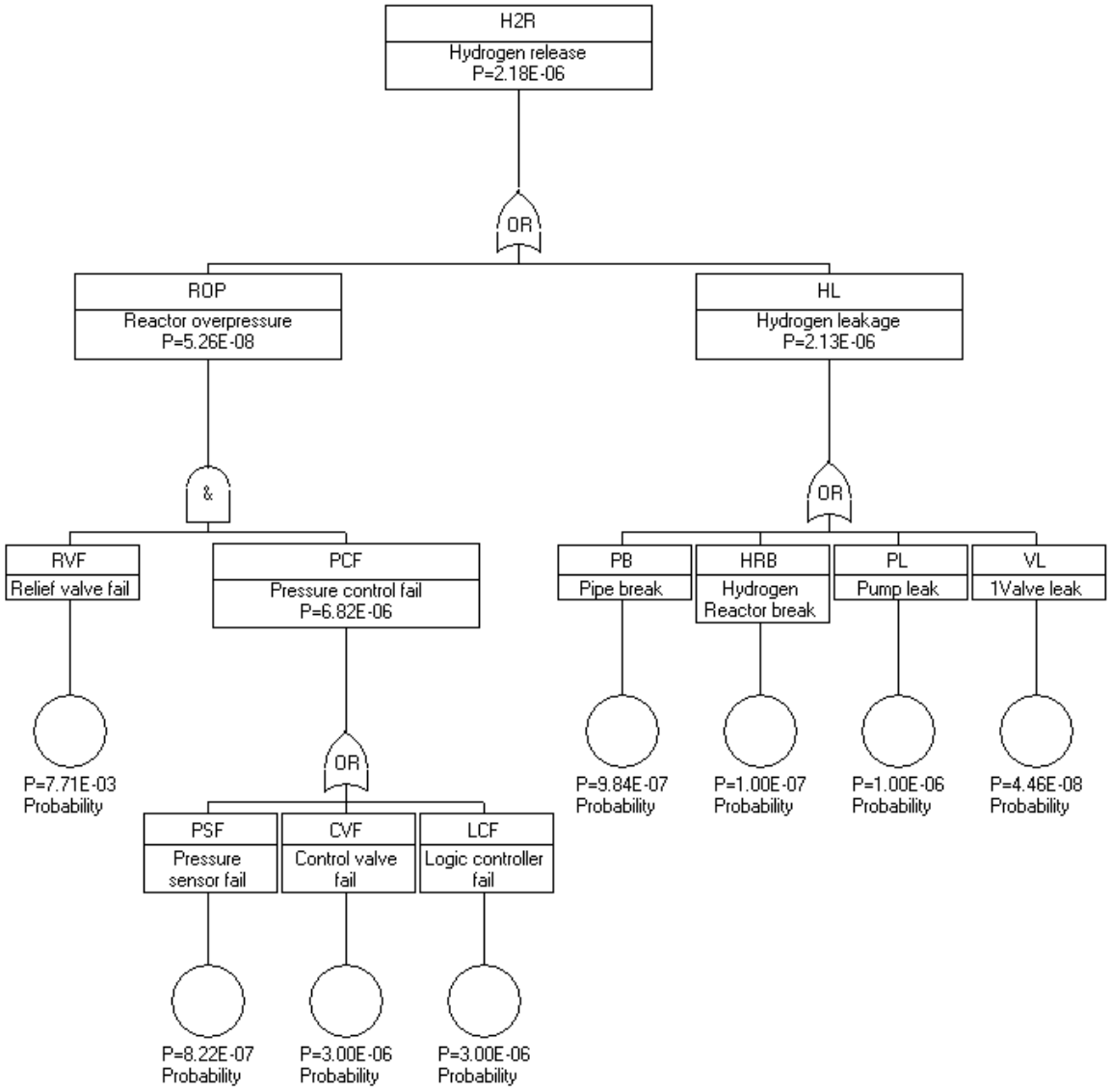


Figure 4.8 Fault tree for hydrogen release

Table 4.2 Failure rate for hydrogen generation

Code	Description	Available values*	Value used	Comment
PSF	Pressure sensor fail	NUREG: 8.22E-7/h	8.22E-07/h	
CVF	Control valve fail	NUREG: 3.0E-6/h	3.0E-06/h	Fail to control
LCF	Logic controller fail	WSRC: 3.0E-6/h	3.0E-06/h	
RVF	Relief valve fail	NUREG: 7.71E-3/d	7.71E-3/d	Failure per demand
PB	Pipe break	NUREG: 6.89E-10/h-ft E&R: 3.0E-9/h-ft	9.84E-7/h	100m
HRB	Hydrogen reactor break	WSRC: 1.0E-7/h	1.0E-7/h	Pressurized tank
PL	Pump leak	WSRC: 1.0E-6/h	1.0E-6/h	External leak
VL	Valve leak	NUREG: 4.46E-8/h E&R: 1.0E-8/h	4.46E-08/h	

**NUREG: NUREG/CR-6928 Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants.*

E&R: Component external leakage and rupture frequency estimates.

WSRC [61]*: WSRC-TR-S3-262 Savannah river site generic data base development (u).*

The initiating event probability of hydrogen release is 2.18E-6/h, and converted to a frequency of critical year it is 1.9E-2/y. From FTA, the hydrogen leakage in the piping and equipment contributes the most part of probabilities to cause a hydrogen release. While the risk of hydrogen release due to reactor overpressure is effectively mitigated by the relief valve.

4.3.3 ETA for Hydrogen Accidents Sequences

The sequences of a hydrogen leakage are modeled with the event tree as shown in Figure 4.9. The hydrogen release event is selected as an initiating event for the ETA, and a frequency of 1.9E-2/y is assigned to it according to the FTA result. It is assumed hydrogen will continuously release to the environment, until an accidental fire and explosion occurs. The event tree is adopted from Bevi [62]. The classification of flammable substances defined by Bevi is shown in Table 4.3. The assessment is based on worst case scenario, where the hydrogen release occures with the peak hydrogen generating rate as 3.6 kg/s [63].

Table 4.3 Classification of flammable substances [62]

Category	WMS category	Limits
Category 0	Extremely flammable	Liquid substances and reparations with a flash point lower than 0 °C and a boiling point (or the start of a boiling range) less than or equal to 35 °C Gaseous substances and preparations that may ignite at normal temperature and pressure when exposed to air.
Category 1	highly flammable	Liquid substances and preparations with a flash point below 21 °C, which are not, however, extremely flammable.
Category 2	Flammable	Liquid substances and preparations with a flash point greater than or equal to 21 °C and less than or equal to 55 ° C.
Category 3		Liquid substances and preparations with a flash point greater than 55 °C and less than or equal to 100 °C.
Category 4		Liquid substances and preparations with a flash point greater than 100 °C.

Hydrogen is extremely flammable gas. So, according to the classification criteria decribed in Bevi, hydrogen is classified as category 0 material. As a category 0 gas, the direct ignition probability given a hydrogen release is 0.2 with a rate less than 10 kg/s. If a direct ignition does not happen, a flammable cloud is formed due to the continuous hydrogen release and a delayed ignition would take place. The probability of delayed ignition defined in Bevi is $1\text{-}P_{\text{direct ignition}}$, which equals 0.8 in this case. Because the hydrogen is lighter than air, if a delayed ignition doesn't happen either, the released hydrogen will disperse to open atmosphere. The hydrogen release has no harm in this scenario. In contrast, if a delayed ignition occurs, the outcomes of the event would be an explosion or a flash fire based on other condition in the delayed ignition, which can lead to worse result than a early fire. The conditional probability of an explosion is 0.4 given a delayed ignition, and the probability for flash fire is 0.6.

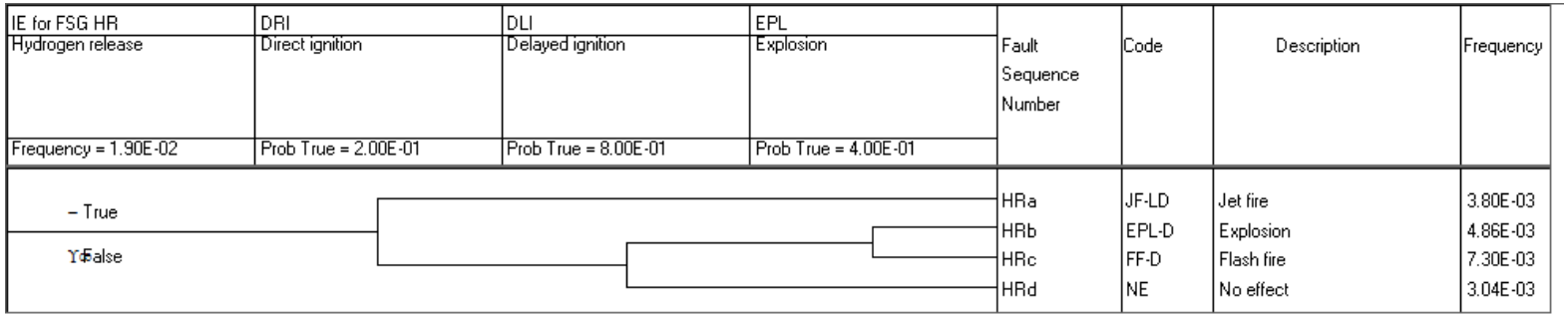


Figure 4.9 Event tree for hydrogen release

The NE state means no harmful effect is given, which has a probability of 3.04E-3. In this accident scenario, neither the direct ignition nor delayed ignition occurs, so the released hydrogen will eventually disperse to the environment. The hydrogen plant is kept safe even a hazardous event is happening. Limited damage would be made from a jet fire (JF-LD), which is caused by hydrogen ignition in early release stage. It is assumed the emergency response action, such as fire extinguishing and emergency shutdown, will stop the release and prevent the hydrogen plant from further harm. The worst case is the explosion (EPL-D) and flash fire (FF-D), when large amount of hydrogen is released and a final ignition occurs. The outcome frequency in the hydrogen release event is summarized in Figure 4.10.

Outcome Code	Outcome Description	Outcome Frequency
EPL-D	Explosion	4.86E-03
FF-D	Flash fire	7.30E-03
JF-LD	Jet fire	3.80E-03
NE	No effect	3.04E-03

Figure 4.10 Summary of hydrogen release outcomes

The outcome distribution for hydrogen accidents is shown in Figure 4.11. Given a hyrogen release condition, there is only 16% chance to avoid an accident. In more than 60% hydrogen release case, a severe hydrogen accident will occur in delayed ignition.The hydrogen release is the major risk in a nuclear-based hydrogen generation system. The safety management for hydrogen accident with SIS will be discussed in the next chapter.

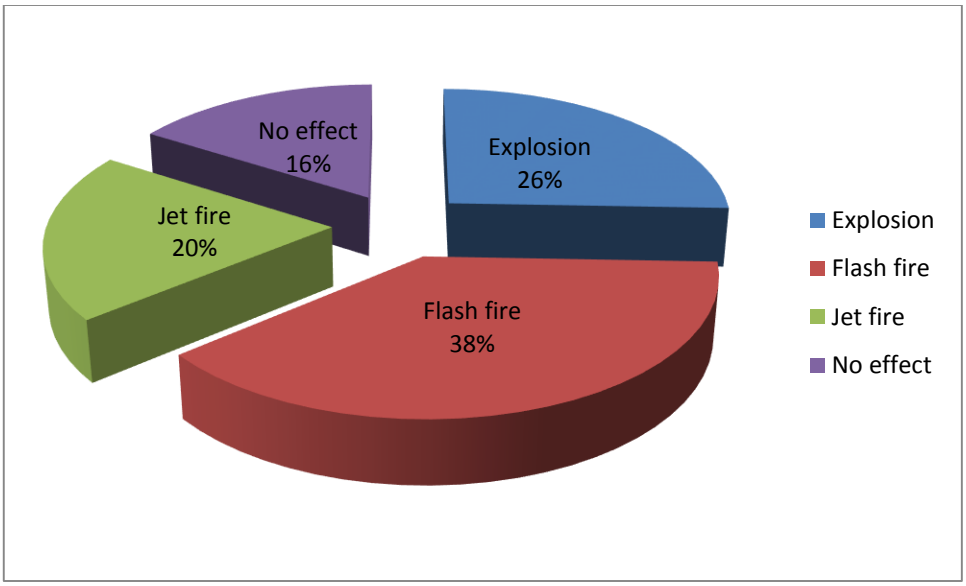


Figure 4.11 Hydrogen accident distributions

4.4 Summary of the Safety Assessment Result

A PSA for nuclear-based hydrogen generation with Cu-Cl cycle has been carried out in this chapter. Two major safety challenges caused by the linkage of the nuclear reactor and the hydrogen generation plant, LOCA and hydrogen accident, are analyzed with PSA- base methodology. The frequency of initiating events, which potentially lead to the final accident in the nuclear-based hydrogen generation system, is evaluated with the FTA. The probability of LOCA is 1.27E-2/y and the probability of hydrogen release is 1.90E-2/y Based on the result derived from FTA, the accident scenarios are modeled with event tree model. The ETA takes the system response into consideration when modeling the accident sequences. The nuclear reactor core damage probability is 4.69E-9/y, which means the

nuclear accident is not the major safety challenge for the system safety of nuclear-based hydrogen generation system. The hydrogen accident has a much higher probability, which is 4.86E-3/y for explosion and 7.3E-3/y for flash fire. From the PSA-based safety assessment, the risks for nuclear reactor in the heat-exchanging interface are effectively controlled by the nuclear safety system. Thus, the nuclear accident has a small contributor to the total accident in the nuclear-based hydrogen. The major risk within the nuclear-based hydrogen generation system comes from the hydrogen accident. By comparing the PSA result with the CFD result, it is also conclude that the hydrogen accident has limited impact on the safety of nuclear reactor if an enough safety distance is applied. The major risks are constricted within the boundary of the hydrogen facilities.

5 Safety Management of Hydrogen Accidents with SIS

According to the PSA results, the risks due to heat transferring from NPP to hydrogen plant has minor impact for system safety, because the nuclear reactor safety system is able to reduce the LOCA accident. The hydrogen accident is the major risk in the nuclear-based hydrogen production plant. Severe hydrogen accidents including flash fire and explosion have a total occurrence frequency as 1.26E-2/y. In this chapter, the safety management for hydrogen accident with the SIS will be discussed.

5.1 LOPA for Hydrogen Accidents

As discussed in previous chapters, safety is a combination of reliability and consequences of accident, to reduce the risk in a process for a given initiating event, two possible methods can be used. The first option is to reduce the probability of occurrence for the initiating event. This can be done by using better component or modifying the process to improve the reliability of unit and system. Another solution is to reduce the chance for accident sequences to reach an unsafe state. SISs are usually used in this case for risk prevention and mitigation.

A LOPA is applied to determine the requirement SIL as the risk reduction level for SIS. LOPA is a semi-quantitative risk analysis technique, which applies following quantitative hazard identification. In general application, the risks is identified from HAZOP and the

occurrence frequency of initiating event is estimated based on experience. However, in this thesis, the accident frequency is derived from more rigorous quantitative assessment with the FTA and ETA. The ETA results for hydrogen accident frequency is used as the accident likelihood.

The possible independent protection layer for a hydrogen release can include:

- general process design
- basic process control system (BPCS)
- alarms
- operators
- SIS

In the previous safety analysis, performance of the basic design with BPCS has been assessed in quantitative model. Therefore, they do not meet the requirement of independent to be treated as IPL. Hydrogen is colorless and odorless gas, so that it is extremely hard to detect a hydrogen release by human. To get a conservative estimation, it is assumed operators will not give an effective response to stop the hydrogen release. Thus, in this LOPA the SIS is defined as the only IPL against the hydrogen release event.

The mitigation target for different accident severity level is given in Table 5.1 [64].

Table 5.1 Severity levels and mitigated event target frequencies [64]

Severity Level	Consequence	Target Mitigated Event Likelihood
Minor	Serious injury at worst	No specific requirement
Serious	Serious permanent injury or up to 3 fatalities	< 3E-6 per year, or 1 in > 330,000 years
Extensive	4 or 5 fatalities	< 2E-6 per year, or 1 in > 500,000 years
Catastrophic	> 5 fatalities	Use F-N curve

In this study the severity hydrogen accident is assigned as extensive, which requires the risk mitigation target as < 2E-6 per year. The risk reduction factor (RRF) required by the SIS is calculated as RRF=1.26E-2/2E-6=6300, and the PFD_G required for the system is 1.59E-4. According to the IEC 61508 standard, a SIL 3 (1000<RRF<10000) SIF is needed for hydrogen accident risk control.

5.2 SIS for Hydrogen Release

A SIS is an additional protection layer on top of the basic control system to prevent people from process hazard. In order to protect a severe hydrogen accident, the SIS need to detect

the release gas in the early leakage stage and perform a safety integrated function to stop the release process.

In the nuclear-based hydrogen generation with Cu-Cl cycle, hydrogen gas is generated from the electrolyser by water splitting, so it is possible to terminate the release by stopping the hydrogen generation. The reaction in the electrolyser can be stopped by cutting down the voltage supply to the electrolyser. In addition, when an emergency stop is required to be performed in the electrolysis reaction, other reactions in the Cu-Cl loop must be stopped at the same time. The plant level emergency shutdown process is beyond the scope of this thesis. It is assumed the plant shutdown process after the emergency shutdown occurs in the hydrogen generating reaction will be controlled by the basic control systems. Only the single reaction shutdown system for the electrolyser is analyzed in this chapter. The block diagram for the SIS is shown in Figure 5.1.

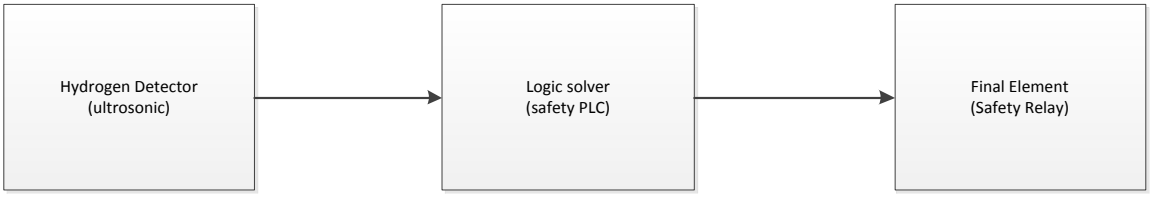


Figure 5.1 SIS block diagram for hydrogen release

SIS usually has the same structure as other control systems but is designed to perform a safety critical function. Similar as other control loops, the SIS consists of 3 parts: the sensors, the logic solvers, and the final elements.

Sensors are the measuring part of SIS. It converts the physical parameter to an electrical signal, which can be read by the logic solver. The logic solver use microprocessors to handle the logic control for the SIS. The logic solver used in SIS is always programmable logic device, which can be configured to meet the requirement for different applications. Final element is the device controlled by the logic solver to perform a designated safety function.

In this SIS design, a safety switch is used as the final element to control the electrical power supply to the hydrogen electrolyser. The operating flow of the SIS in the hydrogen accident is described as follows. In a hydrogen release accident, the release hydrogen gas is concentrated around the electrolyser. When a threshold of hydrogen concentration is reached, the release is initially detected by the sensor and at the same time, a signal will be transferred to the logic solver to indicate a leakage. Then the logic solver working continuously to processing the readings from the sensor, when a leakage is detected, it generates a control signal to stop the hydrogen release by shutting down the electrolysis reaction with the safety switch. If the SIS functions correctly, the hydrogen release can be stopped in the early leakage stage, and the hydrogen generating facilities can be brought back to the safety state before the occurrence of severe accidents.

5.2.1 Sensor: Hydrogen Detector

Hydrogen detector is an essential part of the safety system in the hydrogen generation plant. In the nuclear-based hydrogen generation, plant a wide area hydrogen sensor is required to achieve a plant-wide monitoring coverage range.

There are different types of sensors, which can be used, for wide area hydrogen detection in nuclear-based hydrogen generation system [65], as listed in Table 5.2.

Table 5.2 Comparison of hydrogen detection techniques [65]

Technology	Sensing length (m)	Lowest H2 concentration detected (v %)	Best Response Time (s)	Development Status
Open Path Raman Scattering	50	0.8	<1	Outdoor Demonstration
Distributed Optical Fiber	Sensor: 1 Fiber Length: 880	0.5	2-5	Laboratory System
Ultrasonic	8	NA	<1	Commercially Available
Imaging	4	1	<1	Components Only
Networked Spot Sensors	0.1	<0.05	Varies	Field Demonstrated

Among all the hydrogen detection techniques, the ultrasonic sensor has been proven in use in chemical process, which makes it a promising solution for hydrogen leakage sensing in nuclear-based hydrogen generation system. In the SIS designed to control hydrogen accidents, the ultrasonic sensor is use as the detector.

Hydrogen release from pipe and valves produces ultrasonic turbulent pressure fluctuations. The gas release sensors are designed to receive and analysis these audio signals and detect a sudden ultrasonic signal from the background signals generated by process equipment. A commercially available sensor is shown in Figure 5.2, which is installed above pipe and equipment in a chemical plant [65].

5.2.2 Logic Solver: Safety PLC

Safety programmable logic controllers (PLC) are usually used as logic solver in SIS. The safety PLC plays the functions in a control loop as same as the functions played by conventional PLCs. However, the design and application of safety PLC has two critical safety objectives, which make it different from conventional PLC.

- A safety PLC is designed to have a low failure rate, which makes it has a higher reliability than conventional PLCs.

- If a failure cannot be avoid, the Safety PLC is designed to fail in a safety way.

Figure 5.2 Ultrasonic leakage detector [65]

5.2.3 Final Element

Final element is used to perform the control functions to the system under control. Based on the application requirements, different types of final element can be used, such as actuators, valves, relays, or switches. In the hydrogen release protection SIS, a safety relay is used as the final element. The safety relay is installed in the main circuit of voltage

supply for the electrolyser. When a hydrogen release is detected, the logic solver will send a control signal to the safety relay to cut off the power for hydrogen reaction.

5.3 SIL Calculation for SIS

From the requirement of IEC 61508, the SIL of any SIS must be quantitatively determined to ensure the risk reduction level which can be achieved by the SIS. To demonstrate the safety improvement of nuclear-based hydrogen generation system by using the SIS, a SIL calculation is given as a numerical example for safety assessment. It should be noticed that the purpose of this the example is for the purpose of demonstration. The result shown in this thesis is derived from simplified case study for SIS application in nuclear-based hydrogen generation. The design and assessment of a real application is more complex than the process shown in this paper.

5.3.1 Safety Parameter for Components

The safety parameters (failure rate) for components in SIS are shown in Table 5.3. The value shown in the table is used to demonstrate the calculation process for SIL.

Table 5.3 Component failure rate

Component	Dangerous failure rate λ_D per hour	Detected dangerous failure rate λ_{DD} per hour	undetected dangerous failure rate λ_{UD} per hour
Sensor	3.84E-6	3.77E-6	7.04E-8
Logic Solver	2.26E-6	2.26E-6	7E-9
Final Element	5E-8	1E-8	4E-8

5.3.2 Component PFD_G Calculation

First let us assume a 1oo1 (1 out of 1) configuration for each component. For single element loop, the PFD_G for the subsystem can be calculated with Equation 3.2 and 3.3.

$$\mathrm{PFD}_{\mathrm{G,\,lool}} = (\lambda_{DU} + \lambda_{DD}) \bullet t_{CE} = \lambda_D \bullet t_{CE} \tag{3.2}$$

Where:

$$t_{CE} = \frac{\lambda_{\mathrm{DU}}}{\lambda_{\mathrm{D}}}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{3.3}$$

In the calculation, the proof test interval is 1year (8760 hour) and MTTR is 8 hour. The average PFD for each part is derived with the value listed in Table 5.3, which gives:

- PFD_S of Sensor: 3.39E-04

- PFD_L of Logic Solver: 4.87E-5

- PFD_{FE} of Final Element: 1.76E-4

From equation 3.4, the overall average PFD for the SIS is $PFD_G = PFD_S + PFL_L + PFD_{FE} = 5.15E\text{-}4$.

Form the numerical evaluation, the PFD_G for the 1oo1 system satisfies the SIL 3 requirement for risk reduction level with SIS. However, according to the previous analysis, the maximum allowed average PFD for the SIS must be no greater than 1.59E-4 to achieve the efficient mitigation likelihood target. Thus, according to the SIL assessment result, the 1oo1 loop cannot meet the requirement for the risk reduction in protecting hydrogen release. Redundancy must be used to improve the system reliability.

The system block diagram of the SIS with redundancy is shown in Figure5.3.

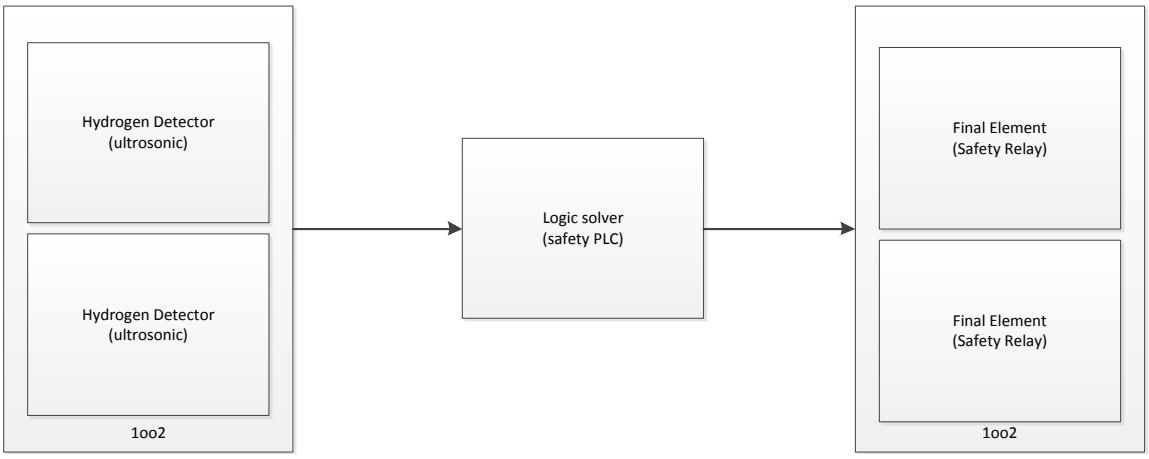


Figure 5.3 SIS with redundancy

As calculated with the simplified equation, the sensor and the final element have higher average PFD, which means the sensor and the final element is the weakness of safety in the SIS designed to control hydrogen accident. To improve the system safety for the SIS design, 1oo2 (1out of 2) channels with redundant components are used to improve the availability of these two subsystems. In a 1oo2 structure, two components are used in parallel and the redundant elements are working independently with each other, so that the system will function correctly if more than one component is working. In other words, the 1oo2 channel is able to tolerate a single fault within the channel.

The PFD_G for 1oo2 system can be calculated with the following equation (Börcsök n.d.).

$$\begin{aligned} \mathrm{PFD}_{G,1oo2} &= 2 \bullet \left(\left(1-\beta_D\right) \bullet \lambda_{DD} + \left(1-\beta\right) \bullet \lambda_{\mathrm{DU}} \right)^2 \bullet t_{CE} \bullet t_{EG} \\ &+ \beta_D \bullet \lambda_{DD} \bullet MTTR + \beta \bullet \lambda_{DU} \bullet \left(\frac{T_1}{2} + MTTR \right) \end{aligned} \tag{5.1}$$

Where

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \bullet \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \bullet MTTR \tag{5.2}$$

And

$$t_{\mathrm{EG}} = \frac{\lambda_{DU}}{\lambda_D} \bullet \left(\frac{T_1}{3} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \bullet MTTR \tag{5.3}$$

In the SIL assessment for 1oo2 loop, the common cause failure value β is taken as 2% and the detected common cause failure is 1%. The average PFD for logic solver and final element are calculated with the value listed in Table 5.3:

- $PFL_{L,1oo2}$ of Logic Solver: 6.22E-5
- $PFD_{FE,1oo2}$ of Final Element: 3.15E-5

The average PFD of the SIS is $PFD_G = PFD_{S,\ 1oo2} + PFL_L + PFD_{FE,\ 1oo2}$=1.46E-4.

According to the SIL assessment result, the SIS with 1oo2 channels of sensors and final element can satisfy the requirement of risk reduction level for SIL 3 system.

The advantages of PSA based approach has been demonstrated from this example. In the general semi-quantitative assessment approach, the previous result (5.15E-4) shows that 1oo1 loop can numerically meet the quantitative requirement for SIL 3 system. However, when combined with a PSA analysis, the result shows that an average PFD of 5.15E-4 cannot guarantee enough mitigation target likelihood. Because the system average PFD is greater than the threshold value (1.59E-4) determined from the PSA assessment approach. Therefore, to effectively reduce the risks for hydrogen accident in the nuclear-based hydrogen generation system, a more reliable SIS is required. By using 1oo2 channels in the sensor and final element subsystems, the system average PFD is improved from 5.15E-4 to 1.46E-4, which is lower than the threshold average PFD requirement. In this application, the uncertainty introduced from the semi-quantitative assessment process is effectively handled and improved by the PSA-based safety assessment approach.

5.4 Software Requirement

The Software requirement is derived with equation 3.15. Given the average PFD limit (1.59E-4) for the mitigation likelihood, the software reliability is PFD_{SW}= (1.59E-4)-(1.46E-4) =1.3E-5. To have potential risks of hydrogen release effectively removed by the SIS, the software component is the SIS must has a reliability higher than 1.3E-5.

A software reliability demonstration test can be performed to achieve the designated software reliability. In industrial field, the 4-20mA current is used as the standard signal. The test cases of software can be simulated with random current input within 4-20mA. Given a confidence level 99% for the test result, the minimal number of executions N with j failures is calculated by solving:

$$\int_0^{F_{sw}} \frac{p^j (1-p)^{N-j}}{B(j+1,1+N-j)} dp \geq C \tag{5.2}$$

Equation 5.2 is an integral equation which can be solved by numerical method (Please see Appendix A). The result is shown in Table 5.4.

Table 5.4 Requirements for SRDT

Numbers of failures, j	Total number of executions, N
0	354241
1	510639
2	646607
3	772697
4	892659
5	1008340
6	1120812
7	1230761
8	1338660
9	1444849
10	1549585
11	1653064
12	1755443

5.5 Summary of Safety Management of Hydrogen Accidents with SIS

In this chapter, a SIS is developed to control the hydrogen accident in the Cu-Cl cycle. First, based on the PSA-based safety assessment result, a LOPA is applied to determine the requirement for the risk reduction level for the hydrogen accident SIS. A SIL 3 grade SIS is designed with the ultrasonic leakage detection sensor. The SIL is calculated for the SIS with the simplified equation to evaluate the safety reduction level of the SIS design. According to the SIL assessment, the 1oo1 loop system configuration could numerically meet the risk reduction requirement for a SIL 3 system. However, after comparing with the PSA result, the 1oo1 SIS configuration is not able to provide the required safety reduction, so SIS with lower PFD must be achieved by modifying the existing design. By using redundancy channel in the sensor and final element subsystem, the new design with 1oo2 sub-channels can get the safety goal for risk reduction. In addition, the quantification of the software safety is also discussed if the software is considered as a part of the SIS safety model.

6 Conclusions and Future works

6.1 Conclusions

Nuclear-based hydrogen generation is a promising technique for large-scale hydrogen production in the future. The linkage of NPP and hydrogen facility introduces new safety challenges for the co-generation plant. To address this problem, an integrated framework of PSA-based safety assessment and management for nuclear-based hydrogen generation system with Cu-Cl thermochemical cycle is developed in this thesis. The PSA-based framework includes the following safety management tasks:

- System identification and problem allocation
- Hazard and risk identification
- FTA for occurrence probability of accidental initiating events
- ETA for the accident sequences
- LOPA to define the requirement of SIL for SIS
- Designing and verification of the SIS

The safety assessment has been carried out based on the early design of Cu-Cl cycle. In the safety assessment, two major safety concerns, LOCA due to direct heat transfer loop and hydrogen accident from Cu-Cl cycle, has been analyzed through PSA-based methods. The PSA study provides a preliminary insight of the plant safety that defines the weakness of

the current design, which needs further improvement. The occurrence probabilities of initiating event, which could cause severe accident in the nuclear-based hydrogen generation system, have been derived from the FTA. The FTA result gives a probability of 1.27E-2/y for LOCA and 1.9E-2/y for hydrogen release. Based on the FTA result, the accident sequences are modeled with ETA to derive all possible outcomes and their probability. The ETA result shows that the nuclear safety issues due to the LOCA in the heat-transferring loop can be handled by the nuclear reactor's safety system, so it has minor impact on the overall safety of nuclear reactor. The hydrogen accident is the major risk in the nuclear-based hydrogen generation plant, which can lead to a severe accident with a probability of 1.2E-2/ year. By comparing the PSA result with the CFD result, it is also determined, that the major impact for hydrogen accident is restricted within the hydrogen generation facilities only.

The SIS is used as an independent protection layer to control and mitigate hydrogen accidents. The LOPA determines that a SIL 3 system is able to reduce the risks of severe hydrogen accident from 1.2E-2/y to 2E-6/y. Two different SIS configurations have been analyzed in this thesis. Although from a conventional assessment approach, a 1oo1 loop can numerically meet the SIL 3 requirement, when fitting into the PSA-based safety management framework, the overall risk reduction (5.15E-4) is not sufficient to guarantee the mitigation likelihood target (1.59E-4). A SIS with 1oo2 redundant channels for the sensor and final element subsystem can meet the safety requirement with average PFD for hardware as low as 1.46E-4 and software reliability no worse than 1.3E-5. The uncertainty introduced from conventional semi-quantitative safety analysis can be addressed by the

quantitative PSA-based approach and achieve a more accurate result to effectively reduce the risks.

6.2 Future Work

In this study, only two major safety challenges, LOPA, and hydrogen accident, in nuclear-based hydrogen plant are analyzed within the PSA-based safety framework. As a complex process, there are many inherent risks in the Cu-Cl cycle, which need further study. A detailed safety assessment for the risks within the Cu-Cl thermochemical process can be performed in the future when more design specifics are available.

The SIS used in this thesis is a simplified case study for the purpose of demonstrating the application of proposed PSA-based safety management framework. The future Cu-Cl hydrogen plant may need an integration of different systems with different control systems and safety systems, which should be more complex in structure and function than the SIS discussed in the thesis. The computer aided design tool is a promising solution for designing complex engineering systems. In the future study, systems automatic optimization design methods can be developed as a potential solution for designing large and complex SIS.

For the energy balance of the nuclear-based hydrogen generation system, the hydrogen plant is working as a load for the NPP. The interaction between the hydrogen generation plant and the NPP should be studied in the future. From the control point of view, during the shutdown and startup, and generation rate changes process of the hydrogen plant,

disturbance will be introduced to the nuclear reactor side through the heat transfer interface, due to the effect of sudden change of reactor external load. In long-term response, the nuclear reactor will balance with the new load in another steady state through a reactor transient response. This load change effect is not deeply investigated in this thesis. This thesis assumes a relative simple system transition case that during the reactor transient response, the basic nuclear control systems are able to maintain the nuclear parameters within the safety range until a new plant balance is achieved. However, as a chemical process, the chemical plant may have different load feature than the conventional turbine generator load. The load balance and control for cogeneration should be further studied with plant modeling and simulation.

7 Bibliography

[1] C. J. Winter, "Hydrogen energy-Abundant, efficient, clean: A debate over the energy-system-of-change," vol. S1, no. 52, 2009.

[2] I. Dincer, "Green methods for hydrogen production," *international journal of hydrogen energy*, vol. 37, no. 2, pp. 1954-1971, 2012.

[3] Z. Wang and G. F. Naterer, "Water Splitting Technologies for Hydrogen Cogeneration from Nuclear Energy," in *Nuclear Power - Deployment, Operation and Sustainability*, INTECH, 2011.

[4] M. Rosen, G. Naterer, R. Sadhankar and S. Suppiah, "Nuclear-based hydrogen production with a thermochemical copper-chlorine cycle and supercritical water reactor," in *Canadian Hydrogen Association Workshop*, 2006.

[5] M. A. Rosen, "Advances in hydrogen production by thermochemical water decomposition: a review," *Energy*, vol. 35, no. 2, pp. 1068--1076, 2010.

[6] C. K. Chow and H. F. Khartabil, "Conceptual fuel channel designs for CANDU-SCWR," *Nuclear Engineering and Technology*, vol. 40, no. 2, p. 139, 2008.

[7] "Reliability vs. Safety," *IEEE Transactions on Reliability*, p. 87, 1981.

[8] US Nuclear Regulatory Commission and others, "Reactor safety study: An assessment of accident risks in US commercial nuclear power plants. Appendix VII, VIII, IX and X," National Technical Information Service, 1975.

[9] IAEA, Procedures for conducting probabilistic safety assessment of nuclear power plants (Level 1), 1992.

[10] IAEA, Procedures for conducting probabilistic safety assessments of nuclear power plants (Level 2) Accident progression, containment analysis and estimation of accident source terms, 1995.

[11] IAEA, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3): Off-Site Consequences and Estimation of Risks to the Public, 1996.

[12] CNSC, RD-337: Design of new nuclear power plants, Ottawa, 2008.

[13] IAEA, Safety of nuclear power plants: design, 2000.

[14] CNSC, S-294: Probabilitistic safety assessment (PSA) for nuclear power plants, 2005.

[15] CNSC, REGDOC-2.4.2: Safety analysis probabilistic safety assessment (PSA) for nuclear power plants, Ottawa, 2014.

[16] CNSC, CNSC Fukushima task force report, CNSC, 2011.

[17] G. Rzentkowski, "Probabilistic safety goals: application to Canadian nuclear power regulation," in *Presentation at 34th Annual Conference of Canadian Nuclear Society*, 2013.

[18] IEC, Functional safety of electrical/electronic/programmable electronic safety related systems, 2000.

[19] IEC, Functional safety: Safety instrumented systems for the process industry sector, 2000.

[20] IEC, IEC 62061 Safety of machinery—Functional safety of safetyrelated electrical, electronic and programmable electronic control systems, 2005.

[21] IEC, IEC Std. 61513 Nuclear power plants-instrumentation and control for systems important to safety-general requirements for systems, 2001.

[22] F. I. Y. Dutuit, A. Rauzy and J. Signoret, "Probabilistic assessments in relationship with safety integrity levels by using fault trees," *Reliability Engineering and System Safety*, vol. 93, no. 12, pp. 1867--1876, 2008.

[23] Y. Liu and M. Rausand, "Reliability assessment of safety instrumented systems subject to different demand modes," *Journal of Loss Prevention in the Process Industries*, vol. 24, no. 1, pp. 49--56, 2011.

[24] H. Jin, M. A. Lundteigen and M. Rausand, "Reliability performance of safety instrumented systems: A common approach for both low-and high-demand mode of operation," *Reliability Engineering and System Safety,* vol. 96, no. 3, pp. 365--373, 2011.

[25] W. Mechri, C. Simon, F. Bicking and K. Ben Othman, "Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment," *Journal of Loss Prevention in the Process Industries,* vol. 26, no. 4, pp. 594--604, 2013.

[26] M. Catelani, L. Ciani and V. Luongo, "A new proposal for the analysis of safety instrumented systems," in *Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International*, 2012.

[27] H. Guo and X. Yang, "Automatic creation of Markov models for reliability assessment of safety instrumented systems," *Reliability Engineering and System Safety,* vol. 93, no. 6, pp. 829--837, 2008.

[28] P. Arun Babu, C. Senthil Kumar and N. Murali, "A hybrid approach to quantify software reliability in nuclear safety systems," *Annals of Nuclear Energy,* pp. 133-140, 2012.

[29] M. C. Kim, S. C. Jang and J. Ha, "Possibilities and limitations of applying software reliability growth models to safety-critical software," *Nuclear Engineering and Technology,* vol. 39, no. 2, p. 129, 2007.

[30] T. Fujiwara, M. Kimura, Y. Satoh and S. Yamada, "A method of calculating safety integrity level for IEC 61508 conformity software," in *Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on*, 2011.

[31] E. Nelson, "Estimating software reliability from test data," *Microelectronics Reliability*, vol. 17, no. 1, pp. 67--73, 1978.

[32] A. Helminen, Reliability estimation of safety-critical software-based systems using Bayesian networks, Radiation and Nuclear Safety Authority, 2001.

[33] M. F. Orhan, B. Dincer and M. A. Rosen, "Efficiency comparison of various design schemes for copper--chlorine (Cu--Cl) hydrogen production processes using Aspen Plus software," *Energy Conversion and Management*, vol. 63, pp. 70--86, 2012.

[34] G. Naterer, S. Suppiah, M. Lewis, K. Gabriel, I. Dincer, M. A. Rosen, M. Fowler, G. Rizvi, E. Easton, B. Ikeda and others, "Recent Canadian advances in nuclear-based hydrogen production and the thermochemical Cu--Cl cycle," *International Journal of Hydrogen Energy*, vol. 34, no. 7, pp. 2901--2917, 2009.

[35] DOE, Nuclear Hydrogen R&D plan, 2004.

[36] M. Piera, J. M. Mar nez-Val and M. Jos Montes, "Safety issues of nuclear production of hydrogen," *Energy conversion and management*, vol. 47, no. 17, pp. 2732--2739, 2006.

[37] DOE, "Feasibility study of Hydrogen production at existing power plants final report," 2009.

[38] C. Smith, S. Beck and B. Galyean, "Separation requirements for a hydrogen production plant and high-temperature nuclear reactor," Idaho National Laboratory, 2005.

[39] S. J. Han and K. I. Ahn, "An investigation of potential risks of nuclear system from hydrogen production," *Nuclear Engineering and Design,* vol. 270, pp. 119--132, 2014.

[40] P. F. Nelson, A. Flores and J. L. Franois, "A design-phase PSA of a nuclear-powered hydrogen plant," *Nuclear engineering and design,* vol. 237, no. 3, pp. 219--229, 2007.

[41] H. S. Kang, "Development of a CFD analysis methodology of H2 explosion accidents for evaluating the safety distance between a VHTR and a H2 productionfacility," 2011.

[42] A. Sully, M. Heitsch, D. Baraldi and H. Wilkening, "Numerical simulations of hydrogen and hydrogen chloride releases in a nuclear hydrogen production facility," *International journal of hydrogen energy,* vol. 36, no. 1, pp. 1083--1093, 2011.

[43] P. F. Nelson, A. Mendoza and J.-L. Franois, "Use of PSA for design of emergency systems in a Sulfur--Iodine cycle," *International Journal of Hydrogen Energy*, vol. 35, no. 12, pp. 6131--6139, 2010.

[44] DOE, MIL-STD-882D System safety program requirements, Washington, 2000.

[45] C. Swann and M. Preston, "Twenty-five years of HAZOPs," *Journal of loss prevention in the Process Industries,* vol. 8, no. 6, pp. 349--353, 1995.

[46] DoD, Procedures for performing a failure mode, effect and criticality analysis, 1980.

[47] US Nuclear Regulatory Commission, NUREG-0492 Fault trree handbook, 1981.

[48] A. Dowell and D. Hendershot, "Simplified risk analysis--Layer of Protection Analysis (LOPA)," in *AIChE 2002 National Meeting*, Indianapolis, IN, 2002.

[49] J. Börcsök, "Comparison of PFD calculation," HIMA Paul Hildebrandt GmbH + Co KG.

[50] J. D. Musa, "Operational profiles in software-reliability engineering," *Software, IEEE,* vol. 10, no. 2, pp. 14--32, 1993.

[51] B. Littlewood and D. Wright, "Some conservative stopping rules for the operational testing of safety critical software," *IEEE Transactions on Software Engineering,* vol. 23, no. 11, pp. 673--683, 1997.

[52] S. Baindur, "Safety issues in nuclear hydrogen production with the very high temperature reactor (VHTR)," in *Canadian Nuclear Society Annual Conference*, Toronto, 2008.

[53] M. Naidin, R. Monichan, U. Zirn, K. Gabriel and I. Pioro, "Thermodynamic considerations for a single-reheat cycle SCWR," in *17th International Conference on Nuclear Engineering*, 2009.

[54] A. J. Lukomski, Study on linking a SuperCritical water-cooled nuclear reactor to a hydrogen production facility, 2011.

[55] Plants, Nuclear Power, Industry-average performance for components and initiating events at US commercial nuclear power plants, Citeseer, 2007.

[56] S. Eide, S. Khericha, M. Calley and D. Johnson, Component external leakage and rupture frequency estimates, Idaho Falls, ID (United States): EG and G Idaho, Inc., 1992.

[57] J. Wolfgong, M. Linn, A. Wright, M. Olszewski and M. Fontana, Systems analysis of the CANDU 3 Reactor, Oak Ridge National Lab., TN (United States): Nuclear Regulatory Commission, Washington, DC (United States). Div. of Systems Research, 1993.

[58] I. Ituen, "Comparing the risk of the pressure tube-SCWR to the CANDU using probabilistic risk assessment tools," McMaster University Library, 2012.

[59] D. C. Hendershot, "Hazardous chemicals peer-reviewed inherently safer design an overview of key elements," *Professional Safety*, vol. 56, no. 2, p. 48, 2011.

[60] M. Lewis and S. Ahmed, "Electrolyzer development in the Cu-Cl thermochemical cycle," FY 2013 Annual Progress Report, 2013.

[61] A. Blanchard, "Savannah river site generic data base development," Savannah River Site (US), 2000.

[62] RIVM, Reference manual Bevi risk assessments version 3.2 - Introduction, National Institute of Public Health and the Environment, 2009.

[63] Z. Wang, G. Naterer and K. Gabriel, "SCWR-hydrogen plant thermal integration," 2011. [Online]. Available: http://www.neimagazine.com/features/featurescwr-hydrogen-plant-thermal-integration/.

[64] W. Gulland, "Methods of determining safety integrity level (SIL) requirements-Pros and Cons," in *Practical Elements of Safety*, Springer, 2004, pp. 105--122.

[65] R. Zalosh and N. Barilo, "Wide area and distributed Hydrogen sensors," in *International Conference on Hydrogen Saferty*, 2009.

8 Appendix Numerical Solution for Equation 5.2

```
result=0:1:1;

for j=0:1:12;



low=1;

high=1000;

N=high;

error=1;

count=1;

while abs(error)>0.00000001

   fun=@(p)        (   (p.^j).*((1-p).^(N-j))  )./beta(j+1,1-j+N);

b=integral(fun,0,0.000013);

error=b-0.99;

N_current=N;

if error~=0;

if abs(error)>0.00000001;
```

```
if error<0;
    low=N_current;


    high=high*2;
    N=high;
end;
if error>0;
    high=(high+low)/2;
    N=(low+high)/2;
end;
end;
end;
count=count+1;
end;
result(j+1)=N_current;
end;
```