

석사 학위논문
Master's Thesis

원자력 발전소에 적용된 안전 등급 네트워크
통신망의 신뢰도 평가에 관한 연구

A Study on Reliability Assessment of Safety-Critical Network
Communication in Digitalized Nuclear Power Plant

이 상 훈 (李 想 勳 Lee, Sang Hun)

원자력 및 양자공학과
Department of Nuclear and Quantum Engineering

KAIST

2016

원자력 발전소에 적용된 안전 등급 네트워크 통신망의 신뢰도 평가에 관한 연구

A Study on Reliability Assessment of Safety-Critical Network
Communication in Digitalized Nuclear Power Plant

A Study on Reliability Assessment of Safety-critical Network Communication in Digitalized Nuclear Power Plant

Advisor : Professor Hyun Gook Kang

by

Lee, Sang Hun

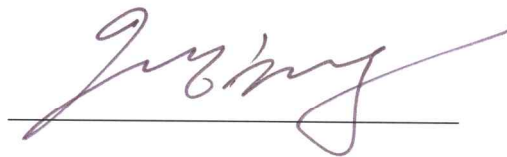
Department of Nuclear and Quantum Engineering
KAIST

A thesis submitted to the faculty of KAIST in partial fulfillment of the requirements for the degree of Master of Science and Engineering in the Department of Nuclear and Quantum Engineering. The study was conducted in accordance with Code of Research Ethics¹⁾.

2015. 12. 10.

Approved by

Professor Hyun Gook Kang

A handwritten signature in purple ink, appearing to read 'Hyun Gook Kang', is written over a horizontal line.

1) Declaration of Ethical Conduct in Research: I, as a graduate student of KAIST, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance of my thesis advisor.

원자력 발전소에 적용된 안전 등급 네트워크 통신망의 신뢰도 평가에 관한 연구

이 상 훈

위 논문은 한국과학기술원 석사학위논문으로
학위논문심사위원회에서 심사 통과하였음.

2015 년 12 월 10 일

심사위원장	강 현 국	(인)
심사위원	성 풍 현	(인)
심사위원	임 춘 택	(인)

MNQE
20143479

이 상 훈. Lee, Sang Hun. A Study on Reliability Assessment of Safety-critical Network Communication in Digitalized Nuclear Power Plant. 원자력 발전소에 적용된 안전 등급 네트워크 통신망의 신뢰도 평가에 관한 연구. Department of Nuclear and Quantum Engineering. 2016. 125 p. Advisor Prof. Kang, Hyun Gook.

ABSTRACT

Recently, the Engineered Safety Feature-Component Control System (ESF-CCS), which uses a network communication system for the transmission of safety-critical information from group controllers (GCs) to loop controllers (LCs), was developed. The use of network communication in control or information transmission system in nuclear power plants (NPPs) provides design flexibility and reduced cost; however, the network communication system has not been applied to ESF-CCS in NPP because the network communication failure risk in the ESF-CCS has yet to be fully quantified.

Therefore, the potential hazardous states and failure mechanisms of network communication between GCs and LCs, which includes High Reliability-Safety Data Link (HR-SDL) and High Reliability-Safety Data Network (HR-SDN), were identified and the quantification schemes for various network failure causes were developed in this study. To quantify the network communication risk and estimate the risk effects of network communication failures in the ESF-CCS, a fault-tree model for engineered safety feature (ESF) components considering the failure of network communication between GC and LC was developed and integrated with OPR-1000 PSA model.

In this study, the hazardous states of network communication were identified both in protocol-level and system-level. To identify the failure mechanisms of network communication which may induce the hazardous states, potential failure causes were analyzed based on the open systems interconnection model of Profibus protocol. The failure mechanisms include hardware failure, software failure, and the failure caused by medium-related bit error. Based on the identified failure mechanisms, quantification schemes for each network failure cause were proposed.

Based on the proposed network communication risk assessment methodology, a fault-tree model for ESF components including the network communication failure in ESF-CCS was developed and integrated with OPR-1000 PSA model. Based on various periodic test intervals for network modules, a sensitivity study was conducted to analyze the risk effect of network failure between GCs and LCs on ESF-CCS signal failure.

Keywords: Nuclear power plant; Digital I&C system; Safety-critical network communication; Fault-tree modeling;

Table of Contents

Abstract	i
Table of Contents	ii
List of Tables	v
List of Figures	vii
Nomenclatures	xi

Chapter 1. Introduction

1.1 Research Background	1
1.2 Literature Review	2
1.2.1 Vulnerabilities of Network Communication in Nuclear Power Plant	2
1.2.1.1 Network Communication Architecture Abstraction	3
1.2.1.2 General Nature of Digital Communication Errors	5
1.2.2 Reliability Assessment of Digital Instrumentation and Control System	6
1.2.2.1 Methods of Reliability Modeling and Assessment of Digital I&C	
Systems	7
1.2.2.2 Integration of the Digital I&C System with a PSA model	8
1.2.2.3 Reliability Modeling of Network Communications in Nuclear Power	
Plant	10
1.3 Objectives and Scope of the Thesis	12
1.4 Organization of the Thesis	13

Chapter 2. Network Communication Systems in Nuclear Power Plant

2.1 Engineered Safety Feature-Component Control System	20
2.2 HR-SDL Network Communication	22
2.2.1 Profibus-FDL Protocol	23
2.2.2 Layout of HR-SDL in ESF-CCS	24
2.3 HR-SDN Network Communication	25
2.3.1 Profibus-DP Protocol	26
2.3.2 Layout of HR-SDN in ESF-CCS	28

Chapter 3. Proposed Framework for Reliability Modeling of Network Communication Systems in Nuclear Power Plant

3.1 Identification of Hazardous States of Network Communication	37
3.1.1 Identification of Hazardous States in Protocol Level	38
3.1.1.1 Token Reception	39
3.1.1.1 Data Transmission	39
3.1.1.1 Data Reception	40
3.1.1.1 Token Passing	40
3.1.2 Identification of Hazardous States in System Level	40
3.2 Identification of Failure Mechanisms of Network Communication	42
3.2.2 Failure Mechanisms in Physical Layer	43
3.2.3 Failure Mechanisms in Data link Layer	44
3.2.3 Failure Mechanisms in Application Layer	45
3.3 Quantification of Network Failure Mechanisms	46
3.3.1 Quantification of Hardware Failure Probability	47
3.3.2 Quantification of Software Failure Probability	50
3.3.3 Quantification of Failure Probability related to Bit Error	51

Chapter 4. Development of Fault-tree Model for Network Communication Systems in Nuclear Power Plant

4.1 Analysis of the Signal Flow in ESF-CCS	61
4.1.1 Required ESF signals for Accident Mitigation Actions	61
4.1.1.1 High Pressure Safety Injection System	61
4.1.1.2 Low Pressure Safety Injection System	62
4.1.1.3 Auxiliary Feedwater System	63
4.1.1.4 Containment Spray System	64
4.1.2 Functional Allocation of ESF Components in ESF-CCS	65
4.2 Fault-tree Modeling of Network Communication in ESF-CCS	66
4.2.1 Fault-tree Modeling of HR-SDL Network Communication	66
4.2.2 Fault-tree Modeling of HR-SDN Network Communication	70

Chapter 5. Reliability Assessment of Network Communication

5.1 Sensitivity Study	92
5.2 Analysis of Minimal Cutsets related to Network Failure	93
5.2.1 Minimal Cutset Analysis for HR-SDL Network Communication	94
5.2.2 Minimal Cutset Analysis for HR-SDN Network Communication	96
5.3 Analysis on the Risk Effect of Network Communication Failure	96

Chapter 6. Conclusion 112

Reference 115

요 약 문 (Summary) 123

감 사 의 글 (Acknowledgement) 124

이 력 서 (Curriculum Vitae) 125

List of Tables

Table 1.1 Description of communications-related errors	14
Table 1.2 Description of sender- or receiver-related errors	15
Table 1.3 Comparison of communication error types with the three primary abstraction layers	15
Table 2.1 ESF-CCS data communication specifications	30
Table 3.1 Major operation processes of token bus protocol and corresponding hazardous states for GC and LC in ESF-CCS	53
Table 3.2 Failure rate of various modules in a single GC and LC	53
Table 3.3 Module-level failure rate of HR-SDL communication module	54
Table 3.4 Failure rates for sub-level hardware components in the network module of Profibus-DP controller	54
Table 3.5 Software integrity levels and their corresponding reliability targets from IEC 61508	55
Table 3.6 Definition of consequences described in IEEE Std 1012-2004 regarding software integrity levels	55
Table 3.7 Categories of likelihood of occurrence described in IEEE Std 1012-2004 regarding software integrity levels	56
Table 3.8 Assignment of software integrity levels based on IEEE Std 1012-2004	56
Table 3.9 Typical bit error probability values for various transmission systems	57
Table 3.10 Description of the data in data frame of network communication between a single GC and LC	57
Table 4.1 Mitigation actions regarding initiating events for OPR1000 and their required ESF actuation signals	71
Table 4.2 Description of ESF components and corresponding LC allocation	72

List of Tables

Table 5.1 Test functions of ESF-CCS	99
Table 5.2 Description of sensitivity study cases for periodic test methods and their interval	99
Table 5.3 Dominant MCSs of IE SLOCA CD sequences in case 1. for HR-SDL network communication	100
Table 5.4 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 1. for HR-SDL network communication	101
Table 5.5 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 2. for HR-SDL network communication	102
Table 5.6 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 3. for HR-SDL network communication	103
Table 5.7 Dominant MCSs of IE SLOCA CD sequences in case 1. for HR-SDN network communication	104
Table 5.8 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 1. for HR-SDN network communication	105
Table 5.9 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 2. for HR-SDN network communication	106
Table 5.10 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 3. for HR-SDN network communication	107
Table 5.11 Summary of the risk quantification results for HR-SDL network communication	108
Table 5.12 Summary of the risk quantification results for HR-SDN network communication	108

List of Figures

Figure 1.1 A representative arrangement of modules and network communications in a typical digital protection system	17
Figure 1.2 Network open systems interconnection model	17
Figure 1.3 Typical (non-redundant) communications network topologies	18
Figure 1.4 Typical (redundant) communications network topologies	18
Figure 1.5 Example scenarios for token ring signal loss	19
Figure 1.6 Examples of failure modes and corresponding recovery mechanisms of a typical token ring protocol	19
Figure 2.1 APR-1400 MMIS architecture	30
Figure 2.2 Configuration of NRC DC application design of the APR1400	31
Figure 2.3 Single class-1 master in cyclic communication	31
Figure 2.4 Two masters sharing token for cyclic data exchange with its slaves	32
Figure 2.5 APR1400 NRC DC ESF-CCS functional block diagram	32
Figure 2.6 KNICS ESF-CCS configuration (single division)	33
Figure 2.7 An example of Profibus-DP communication between multiple stations (red line)	33
Figure 2.8 Data exchange mechanism of Profibus-DP protocol	34
Figure 2.9 OSI model for various Profibus network communication protocol ..	34
Figure 2.10 Profibus bus access protocol including token passing protocol between master stations	35
Figure 2.11 Conceptual flow of bits during a data transmission on a token ring network	35
Figure 2.12 Layout and signal flow of the ESF-CCS	36
Figure 3.1 An example of various service levels of Profibus-DP protocol	58

List of Figures

Figure 3.2 Hardware structure of HR-SDL communication module	58
Figure 3.3 Block Diagram DPC31 (Siemens PROFIBUS-DP Controller)	59
Figure 3.4 Block diagram of general programmable logic controller	59
Figure 3.5 Description of scan process of general programmable logic controller	60
Figure 3.6 Profibus-DP protocol frame structure: (a) token frame format, (b) data frame format with fixed lengths of the data units	60
Figure 4.1 Alignment of ESF components of HPSIS in an injection mode	73
Figure 4.2 Alignment of ESF components of HPSIS in a recirculation mode ..	73
Figure 4.3 Alignment of ESF components of LPSIS in an injection mode	74
Figure 4.4 Alignment of ESF components of AFW system in an operational mode	74
Figure 4.5 Alignment of ESF components of CS system in an injection mode	75
Figure 4.6 Alignment of ESF components of CS system in a recirculation mode	75
Figure 4.7 Logic of ESF-CCS signal failure for V675 in RAS condition	76
Figure 4.8 Logic of ESF actuation signal failure for V675 in RAS condition ..	76
Figure 4.9 Logic of failure to provide input to LC A4A for V675 actuation ..	77
Figure 4.10 Logic of failure to provide input to LC A4B for V675 actuation ..	77
Figure 4.11 Logic of network failure in LC A4A (including HR-SDL hardware component failure)	78
Figure 4.12 Logic of network failure in LC A4B (including hardware component failure)	78
Figure 4.13 Logic of failure of network protocol (data reception failure) by LC A4A through network bus 1 transferred from GC	79

List of Figures

Figure 4.14 Logic of failure of network protocol (data reception failure) by LC A4A through network bus 2 transferred from GC	79
Figure 4.15 Logic of failure of network protocol (data reception failure) by LC A4B through network bus 1 transferred from GC	80
Figure 4.16 Logic of failure of network protocol (data reception failure) by LC A4B through network bus 2 transferred from GC	80
Figure 4.17 Logic of failure of LC A4A input generation by GCs (via network bus 1) in division A	81
Figure 4.18 Logic of failure of LC A4A input generation by GCs (via network bus 2) in division A	81
Figure 4.19 Logic of independent GC failure for V675 actuation (in the case of GC A1)	82
Figure 4.20 Logic of sub-level hardware component failure in network module of GC A1	82
Figure 4.21 Logic of network failure in GC A1 through network bus A1	83
Figure 4.22 Logic of sub-level hardware component failure in network module of GC A2	83
Figure 4.23 Logic of network failure in GC A2 through network bus A1	84
Figure 4.24 Logic of sub-level hardware component failure in network module of GC A3	84
Figure 4.25 Logic of network failure in GC A3 through network bus A1	85
Figure 4.26 Logic of ESF-CCS signal failure for V675 in RAS condition	85
Figure 4.27 Logic of network failure in LC A4A (including HR-SDN hardware component failure)	86
Figure 4.28 Logic of network failure in LC A4B (including hardware component failure)	86
Figure 4.29 Logic of HR-SDN sub-level hardware component failure in network module of GC A1	87

List of Figures

Figure 4.30 Logic of sub-level hardware component failure in network module of GC A2	87
Figure 4.31 Logic of sub-level hardware component failure in network module of GC A3	88
Figure 4.32 Logic of failure of network protocol (data reception failure) by LC A4A through network bus 1 transferred from GC	88
Figure 4.33 Logic of failure of network protocol (data reception failure) by LC A4A through network bus 2 transferred from GC	89
Figure 4.34 Logic of failure of network protocol (data reception failure) by LC A4B through network bus 1 transferred from GC	89
Figure 4.35 Logic of failure of network protocol (data reception failure) by LC A4B through network bus 2 transferred from GC	90
Figure 4.36 Logic of network failure (token transmission) in GC A1 through network bus A1	90
Figure 4.37 Logic of network failure (token reception) in GC A1 through network bus A1	91
Figure 4.38 Logic of network failure (data transmission) in GC A1 through network bus A1	91
Figure 5.1 General cycle of PLC self-diagnostics	109
Figure 5.2 One-top fault-tree model for OPR-1000 nuclear power plant	109
Figure 5.3 Sensitivity study results for the effect of periodic test interval on network failure in case of HR-SDL network communication	110
Figure 5.4 Sensitivity study results for the effect of periodic test interval on network failure in case of HR-SDL network communication	110
Figure 5.5 Summary of sensitivity study results on various periodic test interval	111

Nomenclatures

Abbreviations

ACM	Access Control Machine
AFAS	Auxiliary Feedwater Actuation Signal
AFW	Auxiliary Feedwater
APR-1400	Advanced Power Reactor-1400
ASIC	Application Specific Integrated Circuit
BER	Bit Error Rate
CCF	Common Cause Failure
CDF	Core Damage Frequency
CIAS	Containment Isolation Actuation Signal
CIM	Component Interface Module
CPU	Central Processor Unit
CRC	Cyclic Redundancy Checksum
CSAS	Containment Spray Actuation Signal
DBA	Design Basis Accident
DMA	Diverse Manual Actuation
DPS	Diverse Protection System
ECCS	Emergency Core Cooling System
ED	End Delimiter
EDSN	ESF-CCS Division Status Network
EIDN	ESF-CCS Inter-Division Network
ELCN	ESF-CCS Loop Control Network
ESF	Engineered Safety Function

ESFAS	Engineered Safety Feature Actuation Signal
ESF-CCS	Engineered Safety Feature-Component Control System
ET/FT	Event Tree/Fault Tree
ETIP	ESF-CCS Test And Interface Processor
FCS	Frame-Check Sequence
FDL	Fieldbus Data Link
FLC	Fieldbus Link Control
FMAC	Fieldbus Medium Access Control
GC	Group Controller
HEP	Human Error Probability
HPSIS	High Pressure Safety Injection System
HR-SDL	High Reliability-Safety Data Link
HR-SDN	High Reliability-Safety Data Network
IFM	Interface Machine
I&C	Instrumentation and Control
LANS	Local Area Networks
LC	Loop Controller
LLC	Logical Link Control
LOCA	Loss of Coolant Accident
LOFW	Loss of Main Feedwater
KNICS	Korea Nuclear Instrumentation and Control System
MAC	Medium Access Control
MFLB	Main Feed Line Break
MMIS	Man-Machine Interface System
MOV	Motor-Operated Valve
MSIS	Main Steam Isolation Signal
MSLB	Main Steam Line Break
NPP	Nuclear Power Plant

NRC-DC	Nuclear Regulatory Commission-Design Certification
NS	Next Station
OPR-1000	Optimized Power Reactor-1000
OSI	Open Systems Interconnection
PLC	Programmable Logic Controllers
PPS	Plant Protection System
PRA	Probabilistic Risk Analysis
Profibus-DP	Profibus Decentralized Periphery
Profibus-FDL	Profibus-Fieldbus Data Link
PS	Previous Station
PSA	Probabilistic Safety Assessments
RAM	Random Access Memory
RAS	Recirculation Actuation Signal
RCS	Reactor Coolant System
RMS	Radiation Monitoring System
ROM	Read-Only Memory
RWT	Refueling Water Tank
RxM	Receive Machine
SD	Start Delimiter
SDN	Send Data With No Acknowledge
SG	Steam Generator
SIAS	Safety Injection Actuation Signal
SIL	Safety Integrity Level
SLOCA	Small Loss of Coolant Accident
SRD	Send And Request Data With Reply
TS	This Station
TxM	Transmit Machine
V&V	Verification And Validation

Chapter 1. Introduction

1.1 Research Background

Recently, instrumentation and control (I&C) systems in nuclear power plants (NPPs) have been replaced with digital-based systems. The reason for the transition to digital I&C systems lies in the critical advantages that they offer over conventional analog systems. Regarding conventional analog systems, certain design problems, such as issues related to the susceptibility to extreme environmental conditions, have been identified. Although there have been some design problems, such as inaccurate design specifications and susceptibility to certain environmental conditions, the primary concerns with the extended use of analog systems are the effects of aging, such as mechanical failures, environmental degradation, and obsolescence. Compared to the conventional analog systems, Digital electronics are essentially free of the drift that afflicts analog electronics, so they maintain their calibration better. They have an improved system performance in terms of accuracy and computational capabilities. They have higher data handling and storage capacities, so operating conditions can be more fully measured and displayed [1].

Digital I&C systems typically generate a significant volume of data; the display provides situational awareness to the operators. Network-connected programmable logic controllers (PLCs) allow effective data transmission for the multiple operational function, including safety or non-safety functions, compared to conventional signal transmission components, such as fiber-optic modems and opto-couplers. However, the primary issue of digital data communication in a safety system involves potential hazards, such as partial or intermittent loss of communication, which is a failure to communicate any necessary data when it is needed, and the creation of erroneous information [2]. Therefore, the probability that

a system becomes unsafe due to a network failure must be evaluated to quantify the system risk and to meet the regulatory requirements for safety-related digital systems as well as communication-related requirements such as IEC 61375-1 standard, IEEE standard 603, and IEEE standard 7-4.3.2 [3-5].

Though many activities were carried out in the life cycle of digital systems to ensure a high-quality product, reasonable reliability models are yet not developed along with data for digital systems that are compatible with existing probabilistic risk analyses (PRA) or probabilistic safety assessments (PSA) to assess the risk of NPP operation and to determine the risk impact of digital system upgrades on NPPs [6].

Therefore, the proper PSA framework for assessing the reliability of safety network system should be developed by considering the characteristics of the safety network. In order to estimate the network communication failure risk and the risk effect of network communication failure on the plant risk in a realistic manner, hazard analysis and the identification of paths which might lead a system to an unsafe state are required, as is the probabilistic quantification of each path [7].

1.2 Literature Review

This chapter presents a review of the results found in literature in the areas of network communication systems and their reliability assessment. The identified vulnerabilities of network system is discussed herein. Existing methods for reliability and modeling and assessment of general digital I&C system as well as its integration with in a PRA context are discussed. Also, the review of existing reliability modelling of network communication and their limitations are presented.

1.2.1 Vulnerabilities of Network Communication in Nuclear Power Plant

The network communication is serial in nature but allows messages to be

addressed to many receivers. The network communications are used in safety systems to communicate large blocks of data for applications such as operator consoles, data historians, and post-accident monitors that require bringing many inputs together in a single device. Therefore, protection systems have drawn on commercial standards such as token ring networks and Ethernet [8, 9]. Since general purpose network is not a deterministic message system, thus, it may lead to a potential for uncertain timing between sending and receiving as well as the loss of a message or random generation of messages, commercial network protocols have to be altered or removed to reach the high level of security and testability required for safety system applications. For token-passing networks, it is one of the deterministic network system, thus, the network is under the control of the last token holder.

As shown in Figure 1.1 which shows a typical arrangement of digital components for a channel protection system, the main protection functions are signal input, comparison, voting, and connection to the actuated devices [10]. These four functions are shown implemented in three modules. The modules communicate via a parallel bus in the backplane. The banks of these modules communicate by a serial connection that emulates a backplane. A failure of the communications at any interface within the sequence of modules forming the primary functions may resulting a failure of the channel. Channel failure can be addressed by the redundancy of the channels and the voting scheme.

1.2.1.1 Network Communication Architecture Abstraction

The open systems interconnection (OSI) model for network communications identifies seven layers that function to convey data from source to receiver. The model defines a networking framework for implementing protocols in seven layers. The architecture and detailed functions of the layers are described in Figure 1.2.

Protocols enable an entity in one host to interact with a corresponding entity

at the same layer in a remote host. A message is passed on the source side from layer seven down to layer one to transmit a message from one application to another. Each layer, if present, appends its layer-specific control data as well as a protocol header. These appended data are used to communicate with the corresponding layer on the recipient side. A large amount of control data is transmitted over the physical medium to the receiver in addition to the original message. At the receiver, the message is passed from the Physical layer up to the Application layer, while each layer performs its requested service and removes its specific control data. The Application layer makes the message available to the application process in its original form.

Digitalized NPPs extensively depend on networked communications to transmit data within and among various control and safety systems. The network can be configured as any one of several topologies while the result being successful transmission of data from source to one or more receiver. Network topology refers to the graph properties of the connections among network nodes and includes three types of topologies: physical topology, signal topology, and logical topology [11, 12]. All three types of topologies influence the network's failure modes, fault propagation, and fault handling properties. Typical non-redundant and redundant network topologies are shown in Figure 1.3 and 1.4, respectively.

In case of safety-critical networks, features such as flexibility, handling multiple protocols, and wide area coverage with many nodes are not needed for safety critical systems and are not recommended because these features may lower communications reliability and introduce unpredictable delays in sending messages between nodes. For point-to-point and bus network structure typically used in safety-critical, high-integrity communication, only one, two, and seven OSI layers are used. Some of the lower layers functions can be handled at the Application layer using application-specific methods. Systems conforming to an established protocol, such as Profibus, are more likely to have application independent layers of software

(communication stacks) and hardware (application-specific integrated circuit).

In terms of the reliability of two typical topology used in the safety-critical system, the bus has more complicated operation and more opportunities for common cause failures (CCFs) due to its interconnections with issues such as node addressing, in addition to failure modes, fault propagation, and CCFs due to the shared bus, while point-to-point networking has more limited types of failures modes because there are fewer nodes. Token passing busses are highly visible shared busses that are engineered to approximate the inherent characteristics of a point-to-point network and reduce media access contention and congestion. However, they trade-off response time whereas point to point can run full time and new failure modes such as dropped token and duplicate token are introduced with token passing networks [13]. Figure 1.5 and 1.6 shows some examples of fault scenarios for signal loss and stages of potential ring recovery for various failure modes in a token passing protocol, respectively.

1.2.1.2 General Nature of Network Communication Errors

Communication is about the delivery of information from a source to one or more receivers and the delivery of a response from the receiver(s) to the source, showing how the information was received and used. Therefore, failures and errors can appear in various places along the path from source to receiver. Possible error sources include source-generated errors, errors generated in the communication or transmission channel, receiver-generated errors, and system-wide, component interaction generated errors [10].

In terms of error types, a non-exhaustive list of communication error types has been investigated in previous studies [14, 15]. The errors are divided into two categories according to whether the error is predominantly communication channel related or is associated more with message sender or receiver. These error types also

correspond to the failure modes associated with digital communication systems [16]. Table 1.1 and 1.2 shows the descriptions of the communication-related errors and sender- or receiver-related errors, respectively. In addition, a comparison of error types with the three primary layers of network communication used in digitalized NPP was investigated in previous studies, as shown in Table 1.3 [17]. The analysis shown is not complete but illustrative of the relationship between error categories and the domains of the communication layers.

1.2.2 Reliability Assessment of Digital Instrumentation and Control System

Digital I&C systems represent data internally as discrete values; they are approximations of the analog values that exist outside of the digital elements. discrete representations of analog values may introduce errors, aliasing, or artifacts. In addition, digital I&C systems perform their computations based on an internal clock-the computation process itself is discrete, unlike the continuous computation performed in analog systems.

Therefore, the modeling of the digital I&C systems should additionally account for the complexity for credible predictions of the digital I&C system stochastic performance compared to that of the analog I&C systems. Especially for the network communication system, it is necessary to enumerate and model all failure modes that may occur in all types of network components to understand fully the impact to all devices attached to the network. Also, it is necessary to model the safety devices and auxiliary devices that may affect the network, such as hubs and switches. Other issues that were identified to be relevant to reliability modelling of digital I&C systems are listed as follows:

- Digital I&C systems use combination of software/firmware in information

processing.

- Digital I&C systems rely on sequential circuits. Since they have memory, their outputs may be a function of system history.
- The rate of data transfer is affected by the choice of internal/external communication mechanisms and the communication protocol. This can affect the digital I&C system reliability and robustness.
- Tasks may compete for a digital controller's resources. This requires coordination between the tasks.
- A finer degree of communication and coordination between the controllers is necessary in order to coordinate multiple digital controllers directly and explicitly.
- A digital controller can remain active and not only react to data, but can anticipate the state of the system.
- Tight coupling and less tolerance to variations in operation increases the digital I&C system sensitivity to the dynamics of the controlled physical process.

In spite of the progress over the past few decades in studying the reliability of digital I&C systems, there is no consensus about how the reliability of network systems should be modeled, measured, and predicted. In addition, there are many areas that need to be established.

1.2.2.1 Methods of Reliability Modeling and Assessment of Digital I&C Systems

There exist several methods that can be used to model and assess the reliability of systems. Current PSA analytical tools that assess the safety of safety-critical systems typically involve fault tree analysis, often in combination with

other methods such as event trees, Markov models and reliability block diagrams [18, 19]. The choice of the method depends on the several modelling requirements. The most commonly used methods includes as follows:

- Fault trees and event trees [20, 21]
- Markov models [22]
- Petri nets [23, 24]

While each method is associated with its own advantages and disadvantages, the vast majority of the PSA models that were developed and that still are being developed employ the event tree/fault tree (ET/FT) method.

Since it is desirable to ensure that the probabilistic model of a digital system can be integrated with the conventional PSA model, using the ET/FT method have the advantage of modeling digital I&C systems for existing NPPs because they already have a PRA model developed using the ET/FT method. Regardless of whether a system is analog or digital, if the system executes a control function, its failure may lead to an initiating event, and so can be modeled in a PSA model in terms of the frequency of the basic event. If the system's function is to mitigate initiating events, it is considered as a protection system and is modeled in terms of the probability that it fails to perform its function.

However, the use of digital I&C systems raises several concerns about the capability of the current PSA tools to account for the dynamic interactions between the digital control system elements and the controlled process. For example, software failures, time dependency of unavailability and incomplete independence of various systems [25]. Therefore, efforts must be made to integrate the distinct characteristics of digital I&C systems in the current PSA tools.

1.2.2.2 Integration of the Digital I&C System with a PSA model

Previous studies have investigated on the methods which a model of a digital system can be integrated with an existing PRA model: directly integrating the system model with the PSA model, and integrate the digital system reliability model into the plant PSA model [26].

Since the current PRAs use the ET/FT method, direct integration of the digital I&C system model in conventional PSA model can be achieved by using a fault tree model of the digital system. Nevertheless, this is the most desirable way of integrating a system model with a PSA because it allows all dependencies of the digital system on other systems along with its support systems to be explicitly modeled. Since all the dependencies are explicitly modeled in the logic model of the fault trees and event trees, both qualitative and quantitative results can be obtained directly from analysis of the PSA model.

At the highest level, the system's failure may be modeled in a PSA as a basic event in a fault tree, and this unavailability/unreliability would be used as the probability of failure of this event in the PSA. Use of this approach requires that the inter-system dependencies associated with the digital system, including its support systems, be properly accounted for. Examples of useful results are the minimal cuts sets, and the importance of the basic components of the digital system and of the overall system to the safety of the plant, as measured by a risk metric such as the plant core damage frequency (CDF).

In addition, reliability modeling of the digital I&C system using traditional ET/FT method takes into some considerations in terms of hardware and software used in the digital I&C system.

In terms of hardware digital components, failures of components of the system, even if they are detected, can be considered to be non-repairable [27]. Since the models are developed to assess the frequency of an initiating event, the plant is assumed to be in the mode of power operation. In this mode of operation, it is expected that if some components of the system fail, they will not be repaired

because this activity would likely cause or require a reactor trip. Hence, the plant's staff would wait until the reactor has been tripped for another reason to carry out any needed repair.

In terms of the software of digital I&C system, its failure can significantly impact its associated digital system [28]. Probabilistic parameters for this kind of failure, such as failure rates, also are necessary for quantifying the models. Hence, a method for assessing them is required. However, the technical community has not reached a consensus about a method to be used for this purpose. To address this shortcoming, a range of parameters can be used in the quantification [29, 30]. For example, a range of values for the failure rate of a specific software failure in the models can be employed to quantify the models and study the significance of this failure to each overall model.

1.2.2.3 Reliability Modeling of Network Communications in Nuclear Power Plant

Network communication does not guarantee consistent on-time message delivery. Lost or delayed messages are common in commercial networked communications. A previous study showed how to predict system failures based on the likelihood of message losses in the Ethernet-based network system [31]. In this study, the system failure rate due to the loss of multiple messages in a row was evaluated. The target system uses a collision-based protocol, which introduces randomness into the network system. Such randomness is avoided in the design of safety network systems for NPPs.

However, a plant safety network should be analyzed in a different manner from that used to analyze a commercial network system because a plant safety network is based on a state-based communication system. A state-based communication system is a system that communicates a fixed set of data at regular

intervals. Such system exhibits more predictable performance outside of standard operating conditions compared with commercial network systems at the cost of a less efficient use of communication bandwidth [32].

Several studies were conducted in the area of deterministic network communication reliability assessment such as Profibus. Most of the studies address only the aspects related with the protocol performability or its schedulability analysis during the network operation [33-36]. Other studies were performed to analyze how Profibus behaves in fault scenarios. The ring stability of token passing protocol, or Profibus, was analyzed in the presence of transmission errors which may hit the control frames by modeling discrete time markov chain [37]. Another study modeled the delay of message transmission and the repair of the safety network [38]. The simulation result showed various path of a message and message delay time by differentiating the number of transmission failure. However, the model was focused on the evaluation of the fault tolerance performance, so it must be extended to evaluate the effect of a safety network failure on the system.

Other studies were conducted a fault injection experiments to evaluate Profibus behavior in various fault scenarios. The causes that lead to the ring instability were identified and characterized for their effect both from temporal and probability of occurrence viewpoints [39, 40]. Other studies have investigated outage events, which have a strong impact in message latency times, and consequently in their worst case response time [41]. The study also analyzed the system outage time, station outage time, and bus cycle time based on the experimental analysis within a fault injection framework.

Only a few studies were performed to quantify the network communication failure risk and analyze the risk effects of the network failure in system-level [42-45]. In order to effectively accommodate the huge number of field controllers, the network communication system is used for the safety-critical information transmission from redundant logic controllers to individual equipment controllers in

the protection system of digitalized NPP. In the previous study, data transmission failure caused by network protocol failures was assumed to result in the total loss of safety component actuation control via the protection system [42]. In order to assess the plant risk effect of the digitalized protection system, the fault-tree models were developed and integrated into a plant risk model to obtain the risk information regarding network communication failure.

However, it is notable that the developed model had some limitations on the treatment of network communication protocol failure, such that the network protocol failure were treated as a catastrophic CCF of network modules similar to the software failure in digital I&C system. Since the safety function of the protection system is allocated in redundant channels along with the redundant network bus and multiple field components are allocated to different PLCs to assure the diversity of the protection system, the reliability model of network communication in NPPs must be constructed considering the redundant network system in the protection system along with the failure modes and causes of the network communication.

Other studies include modeling and analysis of communication protocols, sequence controllers, software systems, and communication networks using Petri net [43]. Petri net modeling can be used to directly simulate fault trees by generating minimal cutsets of the translated trees [44]. In addition, dynamic systems can be qualitatively represented by using stochastic Petri nets [45]. However, limitations of Petri nets include that Limitations of Petri nets include that they lead to a combinatorial explosion with the number of states in larger systems. Stochastically interpreted Petri nets cannot be formally proof checked and, thus, the verification process can be difficult and take a long time [46].

1.3 Objectives and Scope of the Thesis

The objective of the thesis is to identify the potential hazardous states for network communication between GCs and LCs and to develop quantification schemes

for various network failure causes. Based on the developed framework, the thesis also demonstrate the extension of fault-tree model to the reliability modeling of network communication in ESF-CCS in digitalized NPP. To estimate the risk effects of network communication failures in the ESF-CCS, a fault-tree model for engineered safety feature components considering the failure of network communication between GCs and LCs was developed and integrated with OPR-1000 PSA model. Based on a various periodic test interval for network modules, a sensitivity study was conducted to analyze the risk effect of network failure between GCs and LCs on ESF-CCS signal failure.

1.4 Organization of the Thesis

The thesis is structured as follows: in Chapter 2, the general introduction to the network communication systems applied in ESF-CCS, including high reliability-safety data network (HR-SDN) and high reliability-safety data link (HR-SDL), is provided. Chapter 3 presents the proposed framework for the reliability modeling of network communication systems which includes identifying the hazardous states of network communication in both protocol-level and system-level. In addition, the failure mechanisms of network communication based on the OSI model of the Profibus protocol were identified and the quantification scheme of each failure mechanism is proposed. In Chapter 4, the application of the proposed framework to the fault-tree modeling of HR-SDN and HR-SDL network communication in ESF-CCS is demonstrated. Chapter 5 provides the results of the reliability assessment of network communication and the analysis on the risk effect of network failure on the core damage frequency based on the results of conducted sensitivity studies. Chapter 6 concludes the thesis and provides recommendation for future research.

Table 1.1 Description of communications-related errors

Types of errors	Description
Corruption	Messages may be corrupted because of errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference
Unintended Repetition	Messages (old) may be repeated at an incorrect time due to an error, fault, or interference.
Incorrect Sequence	Predefined message sequences (such as process variables and time references) associated with a series of messages from a particular source may be incorrect because of an error, fault, or interference.
Loss	Messages may be lost because of an error, fault, or interference. The loss includes both failures to receive and acknowledgment of received message.
Unacceptable Delay	Messages may be delayed beyond their permitted arrival time window. Conditions leading to delays include errors in the transmission medium, congested transmission medium, interference, and delay in sending buffered messages.
Insertion	Messages may be inserted into the communication medium from unexpected or unknown sources. These messages are in addition to the expected message stream. They cannot be classified as Correct, Unintended Repetition, or Incorrect Sequence because the sources are not expected.
Masquerade	Invalid messages may masquerade as valid ones from an expected source. Communication systems used for safety-related applications may employ further checks to detect Masquerade, such as authorized source identities and pass-phrases or cryptography
Addressing	A safety-relevant message, due to a fault or interference, may be sent to the wrong safety-relevant destination. The receiver could treat the message as a valid communication.

Table 1.2 Description of sender- or receiver-related errors

Types of errors	Description
Buffer Overflow	Messages may be longer than the receiving buffer, which results in buffer overflow and memory corruption. Such an overflow could occur at any data layer.
Data Out of Range	Messages may contain data that are outside the expected range for the given data type. Examples are incorrect times and process variables.
Incorrect Ordering	Messages may appear valid, but data may be placed in incorrect locations within the message. The final sequence may be incorrect because of a deviation in the assembly order or incorrect data in the associated memory locations.

Table 1.3 Comparison of communication error types with the three primary abstraction layers

Error Category	Communication layer interaction		
	Physical Layer	Data Link Layer	Application Layer
Corruption	Corruption within the physical media or interface components	Handles or introduces corruption	Message handling flaw can result in corruption
Unintended Repetition		Handles or introduces Unintended Repetition	Applications might send message >1 time due to flaw
Incorrect Sequence		Handles or introduces Incorrect Sequences	Applications might have responsibility for sending some types of messages first
Loss (Deletion)	Loss within the physical media	Flaw could cause loss	Flaw could cause loss

Table 1.3 (Continued)

Error Category	Communication layer interaction		
	Physical Layer	Data Link Layer	Application Layer
Unacceptable Delay	Flaw could cause delay	Flaw could cause delay	Flaw could cause delay
Insertion	Flaw could cause Insertion	Flaw could cause Insertion	
Masquerade	Flaw could cause Masquerade	Flaw could cause Masquerade	
Incorrect Addressing	Connected to the incorrect destination	Sends the message on the wrong communication port	Applications can be responsible for node names that are ultimately translated into network addresses

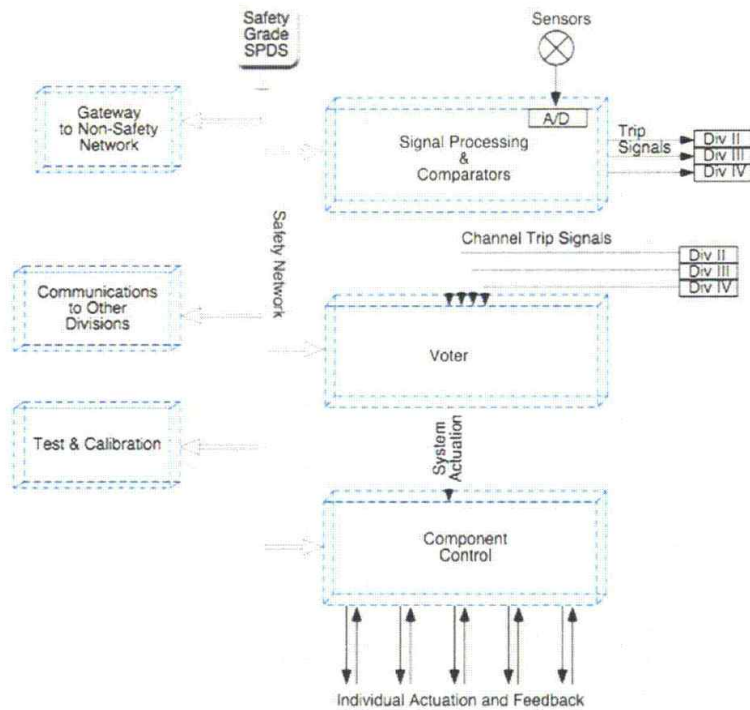


Figure 1.1 A representative arrangement of modules and network communications in a typical digital protection system

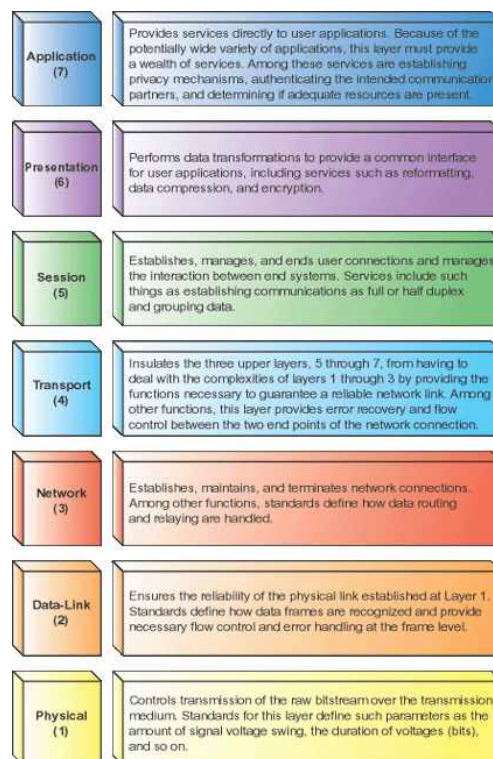


Figure 1.2 Network open systems interconnection model

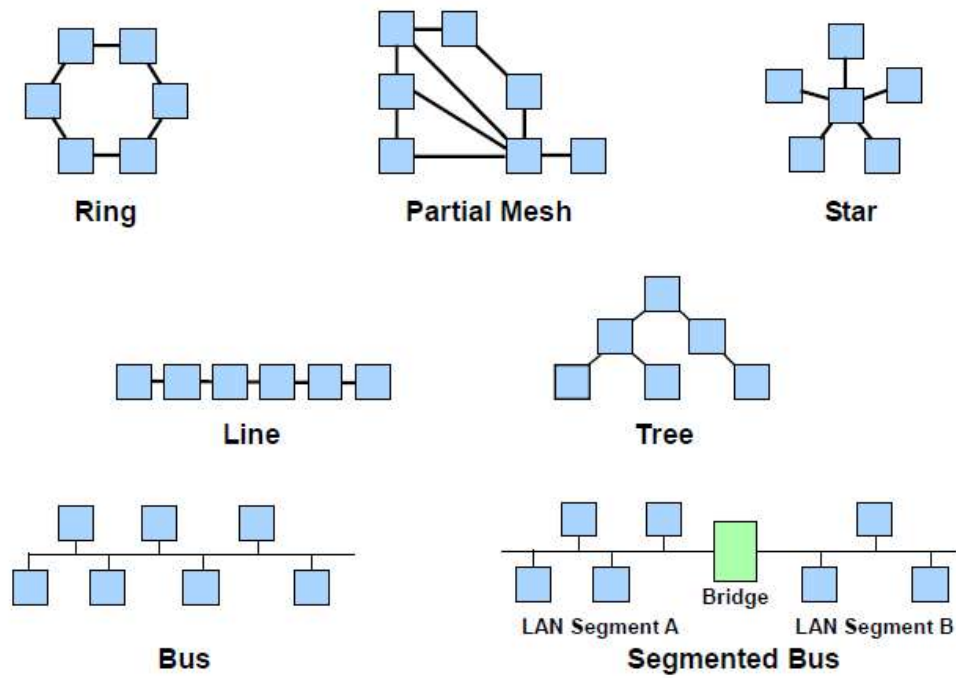


Figure 1.3 Typical (non-redundant) communications network topologies

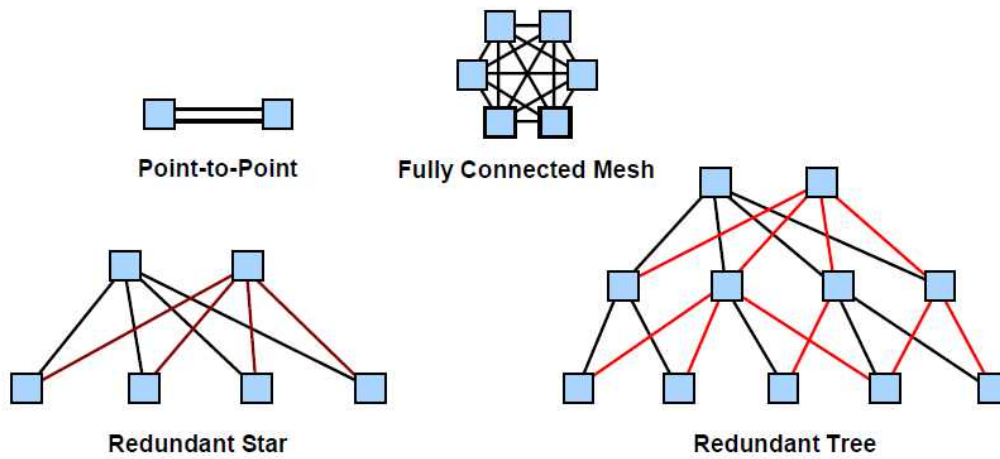


Figure 1.4 Typical (redundant) communications network topologies

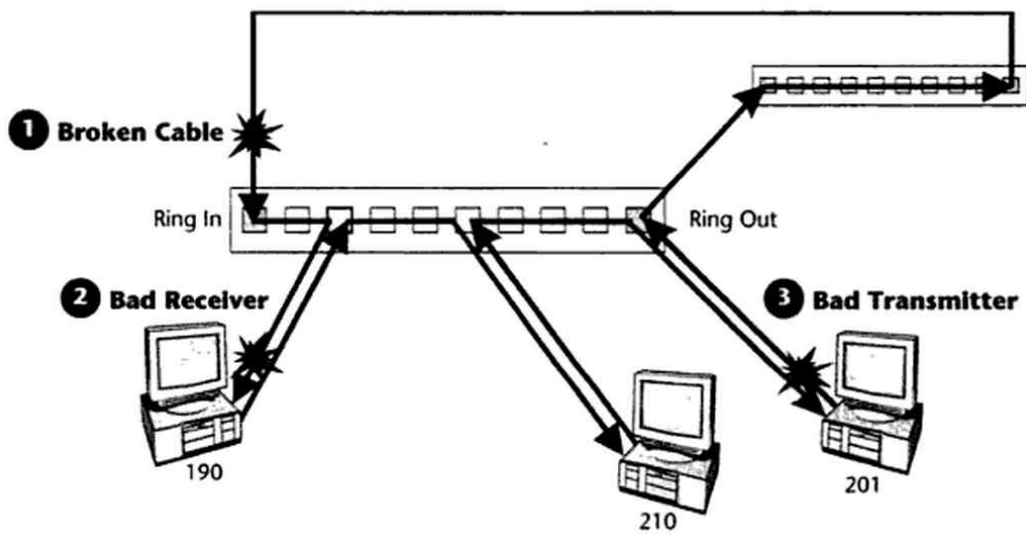


Figure 1.5 Example scenarios for token ring signal loss

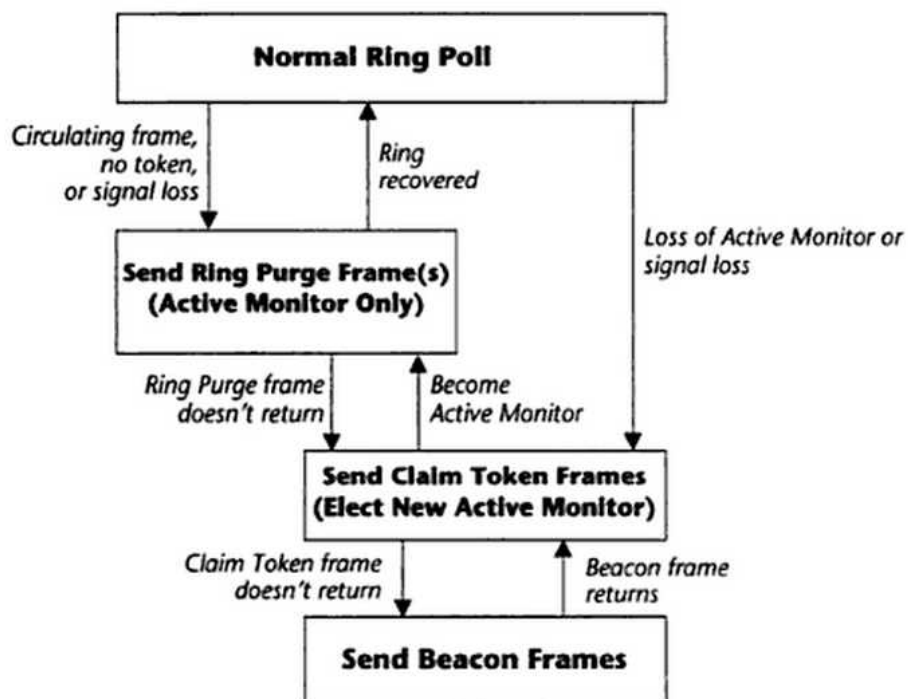


Figure 1.6 Examples of failure modes and corresponding recovery mechanisms of a typical token ring protocol

Chapter 2. Network Communication Systems in Nuclear Power Plant

2.1 Engineered Safety Feature-Component Control System

To achieve technical self-reliance for nuclear I&C systems in Korea, the Advanced Power Reactor 1400 (APR-1400) man-machine interface system (MMIS) architecture was developed by the Korea Atomic Energy Research Institute [2]. This system, which is illustrated in Figure 2.1, is based on a network communication system for both intra-system and inter-system connections. As one of the systems in the developed MMIS architecture, the Engineered Safety Feature-Component Control System (ESF-CCS) employs a network communication system for the transmission of safety-critical information from group controllers (GCs) to loop controllers (LCs) to effectively accommodate the vast number of field controllers.

The ESF-CCS, which initiates several emergency actuations to prevent a plant in a hazardous state during and/or after accidents [47]. Its function is to provide initiating signals for engineered safety function (ESF) components that require automatic actuation when the abnormal conditions are detected. ESF-CCS provides an initiation signal to each of the following independent ESF functions:

- The safety injection actuation signal (SIAS) actuates components necessary for injecting borated water into a reactor coolant system.
- The containment isolation actuation signal (CIAS) initiates the isolation of lines penetrating the containment.
- The containment spray actuation signal (CSAS) initiates the spraying of cool borated water for containment atmosphere.
- The recirculation actuation signal (RAS) initiates the recirculation of

borated water from containment sump.

- The main steam isolation signal (MSIS) initiates the isolation of the two steam generators.
- The auxiliary feedwater actuation signal (AFAS) initiates the supply of auxiliary feedwater to the steam generator when the water level drops to a preset limit.

Basically, the ESF initiation signals are received from the PPS channels and then processed by the ESF-CCS according to the selective two-out-of-four coincidence logic. The output signals are transmitted to the actuated equipment (e.g. pumps, valves, fans, and motors) of the ESF system directly.

The ESF-CCS is designed with four redundant divisions (i.e. A, B, C, and D), and implemented with the safety-graded PLC platform. The principal components of an individual division are fault tolerant GCs, LCs, an ESF-CCS Test and Interface Processor (ETIP), and a Control Channel Gateway (CCG). Each GC receives ESF initiation signals from the RPS and radiation monitoring system via fiber-optic receivers. All GCs perform a system level nuclear steam supply system and balance of plant engineered safety feature actuation signal (ESFAS) logic independently, so that they can transfer the system level ESF actuation signals to all LCs in the division. LCs perform a component control logic using system level ESF actuation signals from GCs or component level control signals from an operator, so that the output control signals are assigned to individual plant components. ETIP takes charge of the passive and active test functions of the ESF-CCS and the interfaces of the ESF-CCS with other systems such as the RPS and qualified indication and alarm system. COM provides information about an ESF actuation status, an ESF component status, a module status, and so on. CCG supports the interface between the ESF-CCS and ESF-CCS soft controllers in the main control room or remote shutdown room.

2.2 HR-SDL Network Communication

In the APR-1400 design which is intended to be used for Nuclear Regulatory Commission-design certification (NRC-DC) application, high reliability-safety data link (HR-SDL) system is employed for providing ESF actuation signal from GCs to LCs, as shown in Figure 2.2 [48]. The ESF-CCS GC receives NSSS ESFAS initiation signals, received from the PPS, and BOP ESFAS initiation signals, received from the safety-related divisional cabinet of radiation monitoring system (RMS). These signals are transmitted via fiber optic SDL to maintain channel independence. The ESF-CCS LC receives ESF actuation signals from the ESF-CCS GC and the component level minimum inventory switch to control safety component. The ESF-CCS performs prioritization of these commands. The output of the ESF-CCS is hardwired to the component interface module (CIM) which performs prioritization of system commands associated with a particular ESF component.

The HR-SDL protocol uses Profibus-Fieldbus Data Link (Profibus-FDL) based on send data with no acknowledge (SDN) [49]. Since HR-SDL is the safety-graded communication module to transmit safety signal such as ESF component actuation, it has the following functions:

- Data flow of the HR-SDL should be in uni-direction and broadcasting method should be used. But, if it is used in the same channel, bi-directional communication is permissible.
- HR-SDL communication module uses deterministic protocol to secure the real time operation.
- Communication protocol of the HR-SDL is composed of minimum function rather than various functions, which should have self-diagnosis and security-authentication functions.

- HR-SDL provide the cycle redundancy check function to confirm the integrity of communication data.
- The Communication data between processor module and HR-SDL shall be exchanged through shared memory without hardware and software interrupt.
- The HR-SDN uses peer-to-peer communication method that communicates through dedicated link, and fiber-optic cable is used as a physical link for physical isolation.

2.2.1 Profibus-FDL Protocol

The layer two protocol is called the Fieldbus Data Link (FDL) layer. there are two sublayers of FDL [50]. The Data Link layer comprises of fieldbus link control (FLC) and fieldbus medium access control (FMAC) sublayers. The FLC provides the interface to the upper layer through various service interface specifications. The medium access control (MAC) sublayer provides a token management finite state machine which takes care of the initialization of the token bus logical ring which comprises of active stations (masters), maintenance of live list which includes the passive stations (slaves) in addition to active stations. The MAC sublayer also handles duplicate token or token loss situations. It is also responsible for adding new (active) stations in the logical ring or deleting faulty masters from the ring.

The FDL system combines two common schemes, master-slave methodology and token passing. In a master-slave network, masters, usually controllers, send requests to slaves, sensors and actuators. The slaves respond accordingly.

Profibus-FDL also includes token passing, a system in which a token signal is passed between nodes [51]. Only the node with the token can communicate. The network can have more than one master. So token passing is used in order to avoid multiple masters talking at the same time. A token is a special message that passes

between masters and carries permission to control the network. The first master initially holds the token and therefore can cyclically communicate with its allocated slaves. But after the last slave has responded, the master must then pass the token over the network to the second master so that it can communicate cyclically with its allocated slaves. When the second master has the token, the first master must remain quiet and must not send any requests. After the last slave has responded to the second master it must pass the token back to the first master so that the cyclic data exchange can proceed. Even if there is one master in our network, it still has a token. A single master will pass the token to itself. Data exchange between the class-1 master and its allocated slaves and token passing between masters is all automatic. Figure 2.3 and 2.4 show the token passing mechanisms for Profibus-FDL network protocol where there is single master station and where there are multiple masters which share the token for cyclic data exchange, respectively.

2.2.2 Layout of HR-SDL in ESF-CCS

Figure 2.5 shows the functional block diagram of ESF-CCS in the APR-1400 design for NRC-DC application [48].

Each ESF-CCS channel receives ESFAS initiation signals from all four channels of the PPS and performs an automatic actuation of the applicable ESF system(s) when certain coincidence logic conditions are satisfied [52]. The ESF-CCS also provides provisions for manual ESF system level actuation and manual component control of ESF components. The 2-out-of-4 actuation logic for voting is performed in the ESF GC 1 and 2 process stations which independently receive ESFAS initiation signals from the four PPS channels (i.e. A, B, C, and D channels) and perform a 2-out-of-4 coincidence voting logic on the initiating signals. Valid ESF system level actuation signals are latched and require manual reset before returning to non-actuation status. Two redundant GCs (i.e. GC 1 and GC2) are

provided for reliability within each ESF-CCS channel.

Based on the outputs of the coincidence logic, the ESF GCs 1 and 2 provide actuation signals to the LCs in the same channel via fiber optic SDLs. Each LC receives the ESF actuation signals from the both ESF GC 1 and 2 and activates the appropriate ESFAS command for the ESF components. The LCs provide discrete ESF actuation signals to the associated CIM. The CIM prioritizes the ESF actuation signals for the component control from the LC, DMA switches, and where applicable, DPS. Any non-discrete components which require modulation are controlled via the analog output module without the CIM.

Error checking techniques such as cyclic redundancy checksum (CRC) are incorporated into the communication protocol to assure the integrity of the transmitted data. Upon detection of the communication loss within a safety system, the system is designed that communication failures shall not prevent safety systems from performing their intended safety function.

2.3 HR-SDN Network Communication

High reliability-safety data network (HR-SDN) system is employed in Korea Nuclear Instrumentation and Control System (KNICS) ESF-CCS loop control network (ELCN), which is used for the transmission of safety-critical data from the GCs to the LCs, as shown in Figure 2.6. Other network system implemented in ESF-CCS, such as ESF-CCS inter-division network (EIDN) and ESF-CCS division status network (EDSN), is used for the transmission of safety-related data, such as test results for voting logic conducted by GCs and LCs during manual testing of the system [53]. Table 2.1 shows the overview of the network communication system implemented in KNICS ESF-CCS.

The HR-SDN system uses the Profibus Decentralized Periphery (Profibus-DP) protocol based on SDN communication; this protocol is a standard fieldbus protocol

that is extensively applied in other industry fields [54]. HR-SDN allows deterministic data communication via Profibus-DP protocol which provides N-to-N safety-critical data exchange and broadcasting via network communication between safety-graded PLCs in ESF-CCS. It supports maximum of 32 stations, such as safety-graded PLCs or computers, in multi-drop fashion. Figure 2.7 shows an example of Profibus-DP application for the network communication between multiple PLCs.

2.3.1 Profibus-DP Protocol

The Profibus-DP communications profile is designed for coupling several stations or actuators (or slaves) to a single controller, using a cyclic polling scheme with only a single master station, as shown in Figure 2.8 [54]. The master station is the only station controlling the medium. In this profile, the layers one (Physical layer) and two (Data Link Layer) of the OSI reference model are covered, as shown in Figure 2.9. In addition, layer seven (Application layer) of the OSI model entities use the link layer interface to obtain services from the link layer.

In terms of the operating mechanism of the Profibus-DP protocol, the protocol that is used for communication is similar to that of the token bus protocol, as shown in Figure 2.10 [37]. The IEEE has established the IEEE 802.4 standard, which specifies the services and a standard for local area networks (LANs) that use explicit token passing schemes to control access on a bus topology network [55].

In the token bus protocol, each station is assigned a location in an ordered sequence, with the last station in the sequence being followed by the first station. The logical topology of the token bus protocol follows a logical ring of active stations via the token passing process, whereas the physical topology follows a bus topology. Because each node only knows the address of its neighbor in the ring, a special protocol is needed to notify the other nodes of connections to or disconnections from the ring. A token bus network employs a small frame, which is

known as a token frame, to grant individual stations exclusive access to the network transmission medium. When a station acquires control of the token frame, it becomes the temporary master of the stations in the ring of the network, and that station is allowed to transmit one or more data frames, depending on the token holding time, which is the time limit imposed by the network. When the station has finished using the token to transmit data, or the time limit has expired, it relinquishes control of the token, and the token is then passed through subsequent stations in the logical topological sequence until the lowest-addressed station acquires the token and passes the token to the active station with the highest address. Figure 2.11 shows the overview of data transmission mechanism for a token passing protocol.

Two types of stations are defined in the Profibus-DP protocol: master stations and slave stations [56]. The master station initiates the message cycle, whereas the slave station sends the acknowledgment or response frame.

A master station forms an "active station" on the network. Profibus-DP defines two classes of masters. A class 1 master handles the normal communication or exchange of data with the slaves assigned to it. A class 2 master is a special device primarily used for commissioning slaves and for diagnostic purposes. Some masters may support both class 1 and class 2 functionality. Master-to-master communication is normally not permitted in Profibus, except in order to grant bus access rights to another master via the exchange of a token. However, master-to-master communication between two mono-master systems can be facilitated. The exchange of bus access rights via this the token ring only applies between masters on the bus.

A slave station is a peripheral device, such as I/O transducer, valve, and network drive, which processes information based on the output from the master stations. The slave station forms a "passive station" on the network since it does not have bus access rights, and can only acknowledge received messages, or send response messages to the master upon request. It is important to note that all slave

stations have the same priority, and all network communication originates from the master.

Compared to the Profibus-FDL which only uses layers one and two of Profibus OSI model, Profibus-DP requires layer seven of Profibus OSI model which is accomplished by application specific integrated circuit (ASIC) and interface modules for connecting master and slave devices to Profibus-DP [57]. Industry-standard SPC3 ASIC are generally implemented in the Profibus-DP protocol and it transfer network data to and from the microcontroller and automatically provide the response to the bus according to the Profibus specification. In addition, it provides services for the software applications needed and the ability for the user to interact with the network [58].

2.3.2 Layout of HR-SDN in ESF-CCS

Figure 2.12 shows the conceptual layout of the KNICS ESF-CCS which consists of data communication between GCs and LCs via network bus [20]. In each division, there are three GCs and up to twelve LCs. Each LC has a hot-standby backup controller. There are two redundant input sources of the ESF-CCS: the plant protection system (PPS) and an operator. If the PPS performs the function successfully, it automatically provides input to the GCs. The human operator could also manually actuate the field components as a backup of an automated system, or PPS, by providing a manual signal to the GCs. The GC performs auctioneering by using four channel outputs from the PPS. If a specific ESF signal is generated based on the auctioneering results, the GC provides information to the LC by using network communication. The GCs' signals are processed in the LCs based on two-out-of-three voting logic. When a LC receives more than two actuation signals, it generates the control signal for the field components in consideration of the characteristics of each component. The control signal for each component is

generated by using a corresponding output module.

If a malfunction of a LC is detected, the hot-standby backup controller will take over the task. The GCs are also monitored by the LCs by using the status monitoring bit of the communication packet. In order to reduce the failure probability of the field components' control signal, there are two more sources in addition to the LC of the ESF-CCS. The diverse protection system (DPS) is an independent and separate automatic system for signal generation. Independent and dedicated sensors provide input to the DPS. The diverse manual actuation (DMA) provides a redundant mean for the operator in the main control room to access the field components via the hard-wired path. It is also notable that the DPS and the DMA switches do not cover all the field components. The DPS generates only AFAS since it has limited number of sensors. Each of these redundancies provides a safety signal to only a limited number of components.

Table 2.1 ESF-CCS data communication specifications

List	Function	Quality		Type
		HW	SW	
EPDL	ESF-CCS ETIP to PPS ATIP	Class 1E	ITS	HR-SDL
ERDL	ESF-CCS ETIP to RMS	Class 1E	ITS	HR-SDL
EDSN	ESF-CCS inter-module data link in single channel	Class 1E	ITS	Profibus-FMS
EISN	ESF-CCS intra-channel data link	Class 1E	ITS	Profibus-FMS
ELCN	ESF-CCS LC data link	Class 1E	SC	HR-SDN
ESCN	ESF-CCS soft control data link	Class 1E	SC	HR-SDN
MCDL	ESF-CCS MCR-CPM to CCG	Class 1E	SC	HR-SDL
RCDL	ESF-CCS RSR-CPM to CCG	Class 1E	SC	HR-SDL

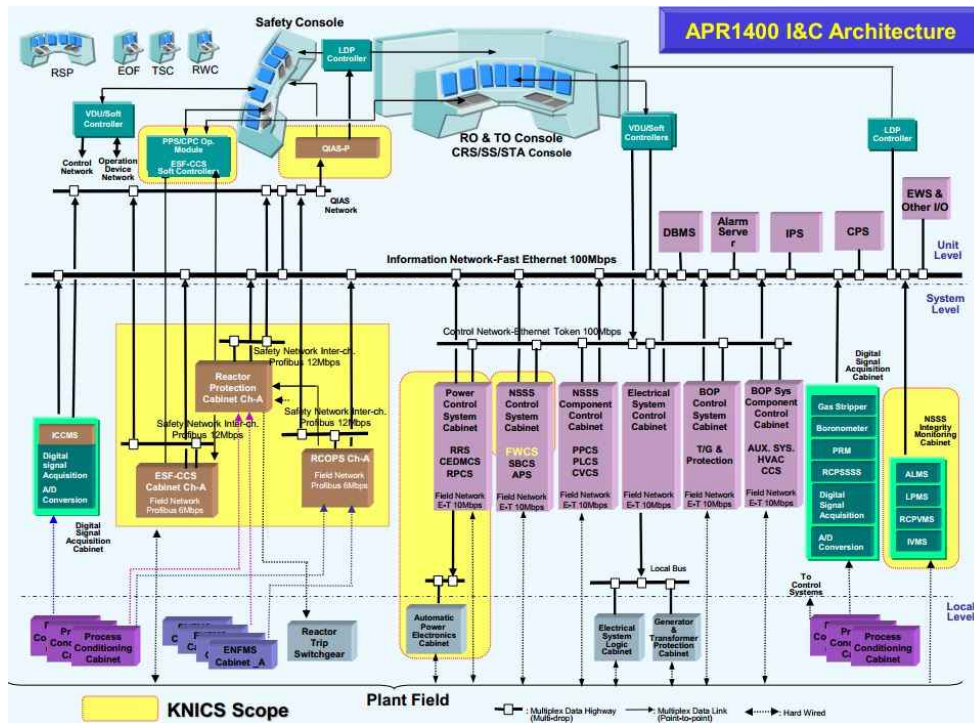


Figure 2.1 APR-1400 MMIS architecture

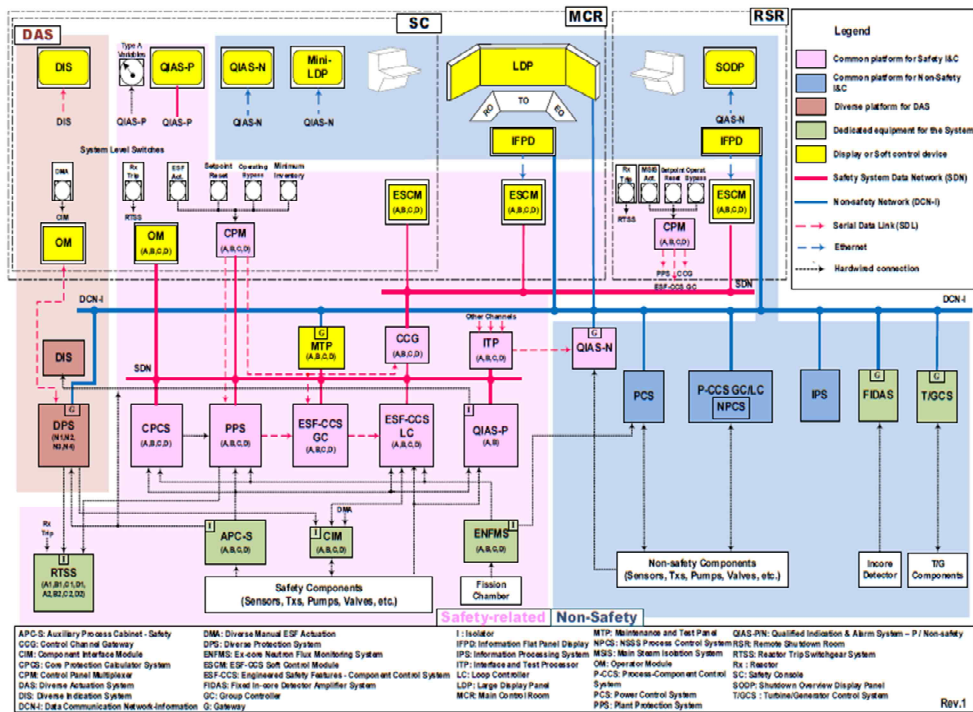


Figure 2.2 Configuration of NRC DC application design of the APR1400

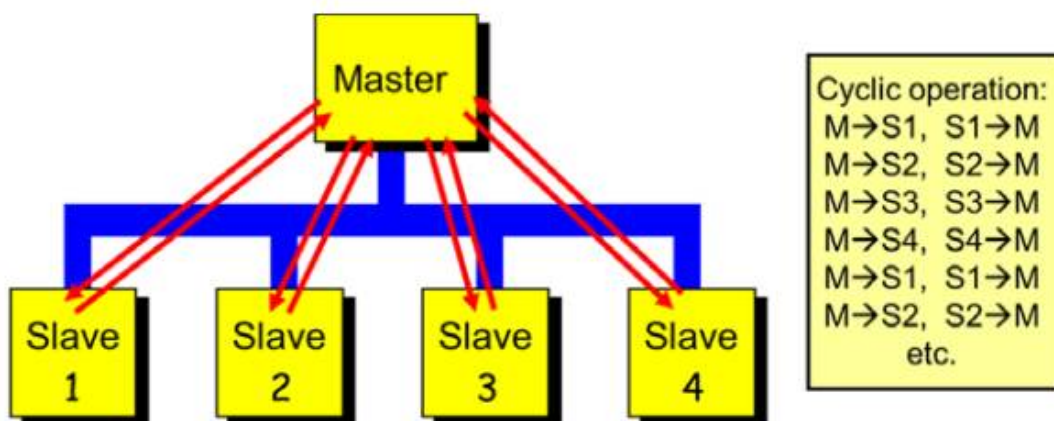


Figure 2.3 Single class-1 master in cyclic communication

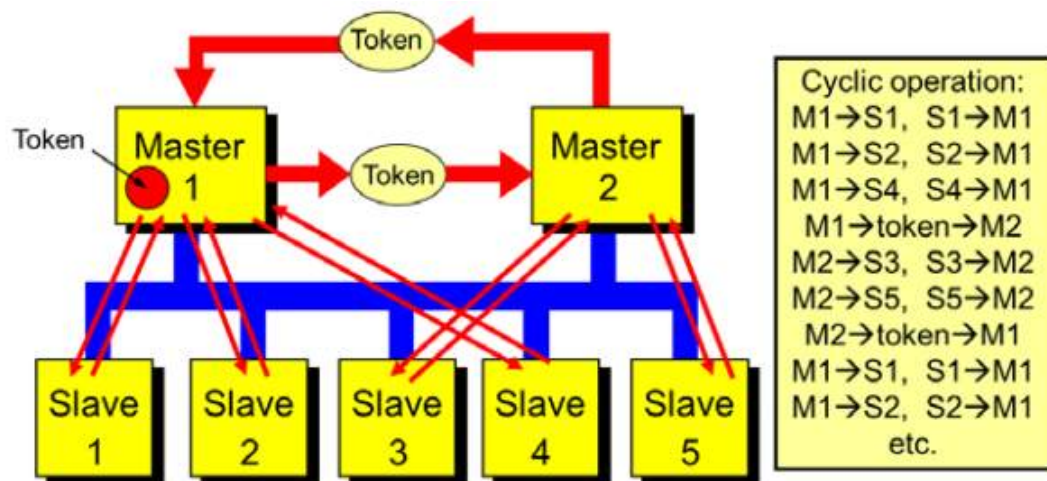


Figure 2.4 Two masters sharing token for cyclic data exchange with its slaves

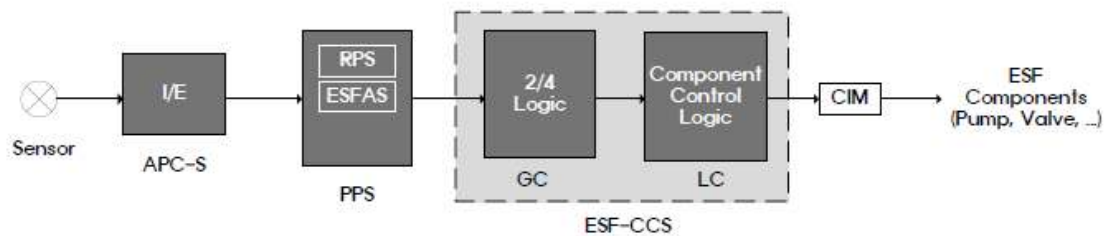


Figure 2.5 APR1400 NRC DC ESF-CCS functional block diagram

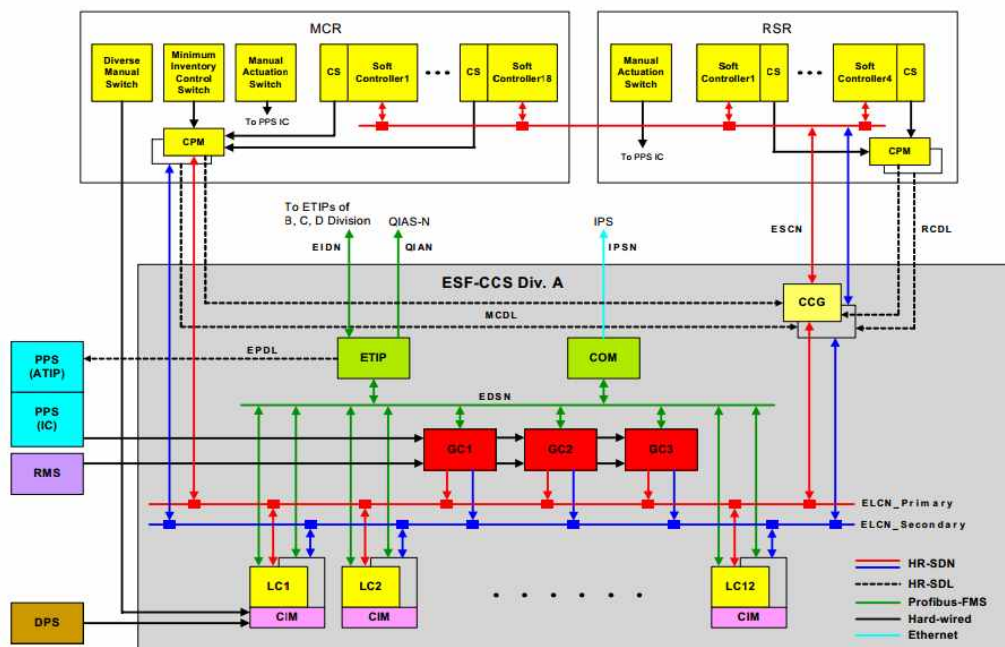


Figure 2.6 KNICS ESF-CCS configuration (single division)

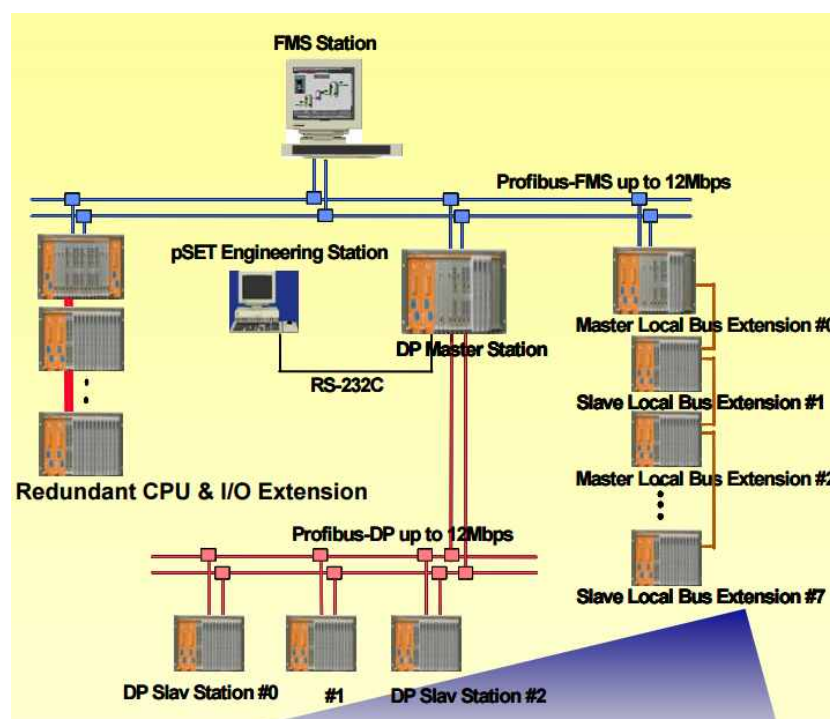


Figure 2.7 An example of Profibus-DP communication between multiple stations (red line)

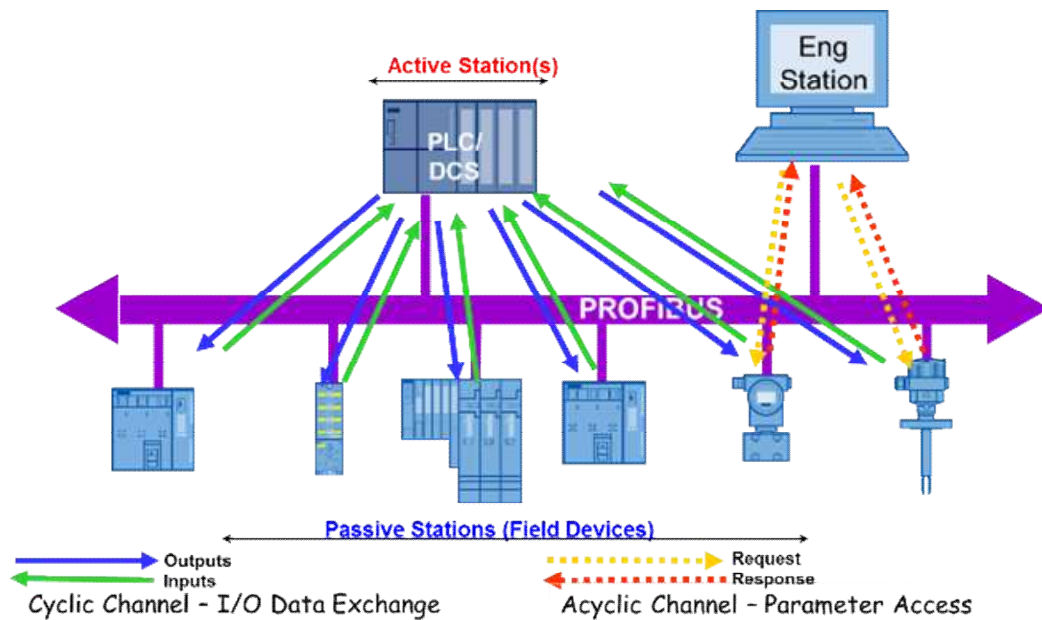


Figure 2.8 Data exchange mechanism of Profibus-DP protocol

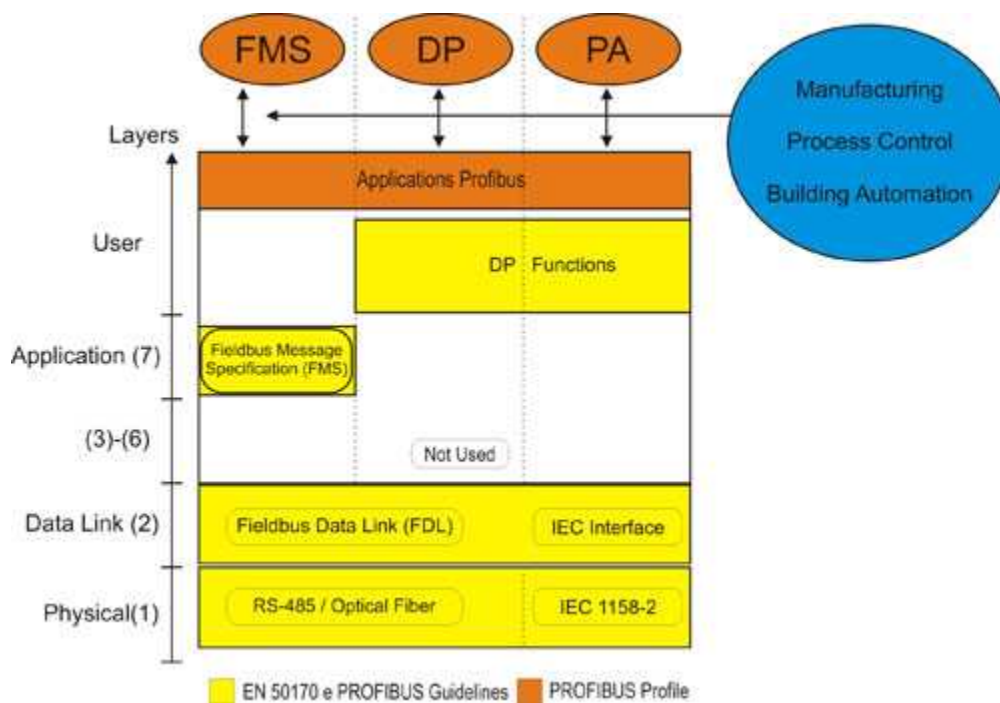


Figure 2.9 OSI model for various Profibus network communication protocol

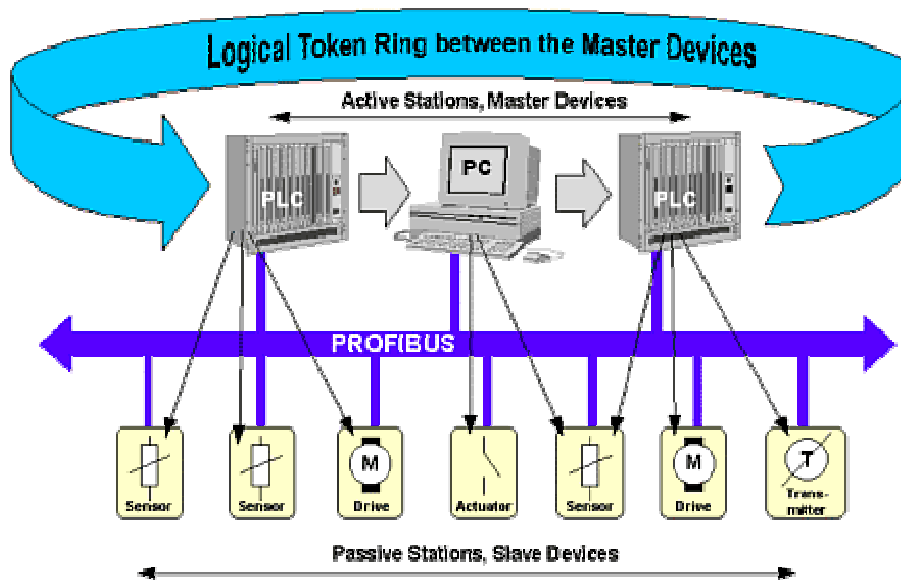


Figure 2.10 Profibus bus access protocol including token passing protocol between master stations

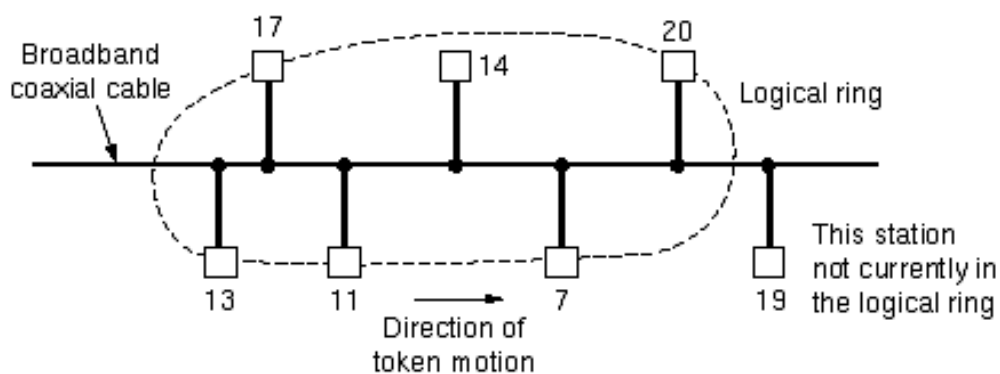


Figure 2.11 Conceptual flow of bits during a data transmission on a token ring network

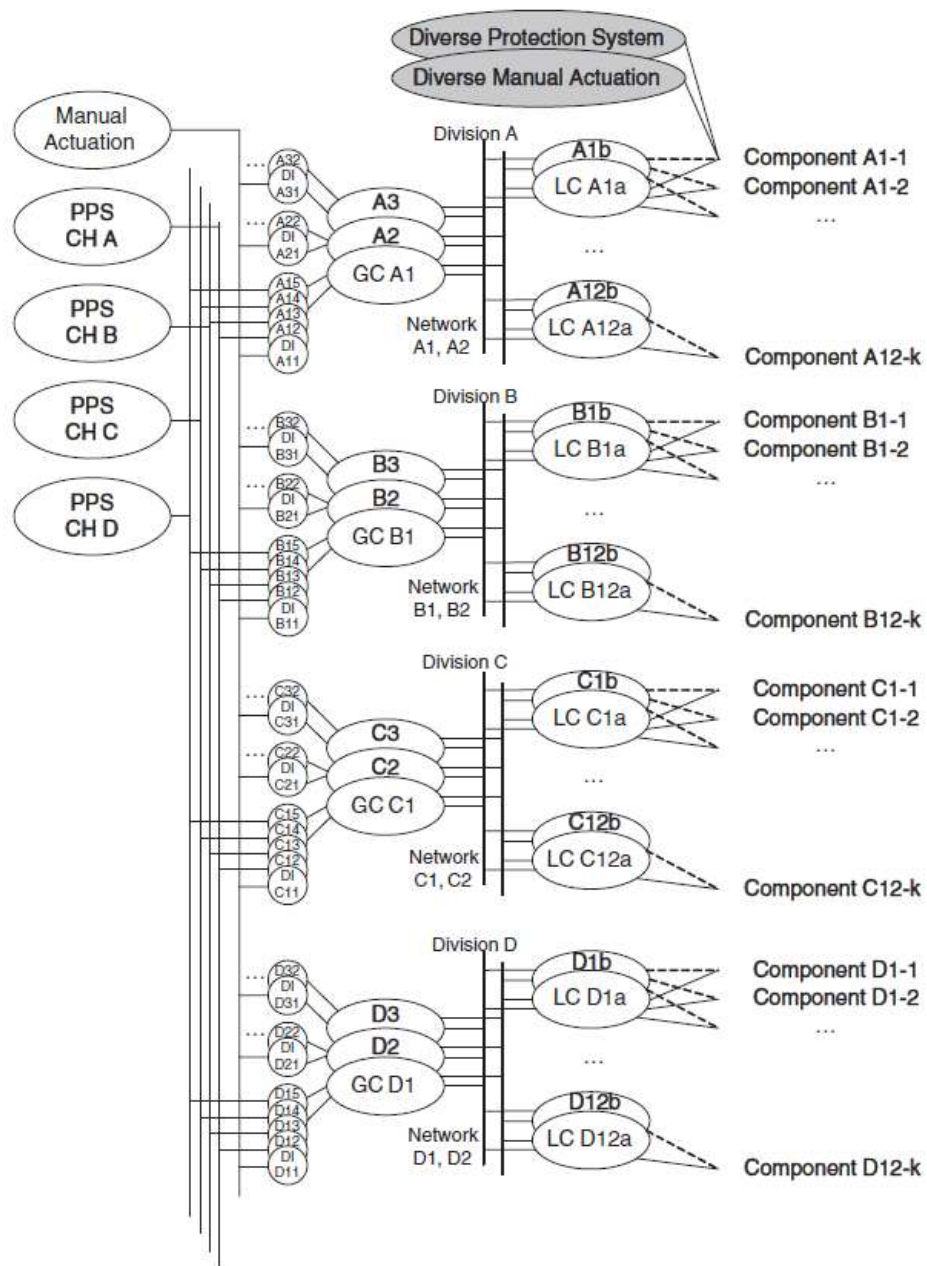


Figure 2.12 Layout and signal flow of the ESF-CCS

Chapter 3. Proposed framework for Reliability Modeling of Network Communication Systems in Nuclear Power Plant

Based on the general operational characteristics of the Profibus protocol, the hazard states and the corresponding causes of failure for network communication between GCs and LCs can be identified. In this study, faults or errors of GCs and LCs are not considered; however, the failure of GCs and LCs, which can terminate the controllers' abilities to perform their functions are considered when assessing the reliability of the target network communication system and the risk effects of network failure between the GCs and LCs on ESF-CCS signal failure [59]. In other words, the error recovery process of the general token bus protocol, including the recovery process by MAC, such as in response to lost or multiple tokens, a token passing failure, a deaf station or stations with duplicate addresses, was not considered because the coverage of these error recovery operations for network failure in ESF-CCS has not yet been investigated.

3.1 Identification of Hazardous States of Network Communication

Application of the network communication technique is useful in reducing the cabling number when a system consists of many components and processor modules. The use of signal transmission components, such as fiber-optic modems and opto-couplers, is reduced by using network communication.

However, safety network communication in the safety-critical system must be evaluated and proved, even though the technique provides many advantages for system development. In order to evaluate the probability that the system becomes unsafe due to network failure, hazard states and the identification of paths which might lead the system to an unsafe state must be identified [59]. In addition, network configuration and hazard states should be reflected and carefully modeled in

a safety assessment model to quantify the risk. In this study, the hazardous states of network failure were identified in both protocol level and system level.

3.1.1 Identification of Hazardous States in Protocol Level

The operation mechanism of the Profibus protocol can be categorized into four major processes: token frame reception, data frame transmission, data frame reception and token frame passing [60]. When one of the above network communication process is failed, GCs fail to transmit safety-critical information to LCs, thus, the system can enter hazardous state which is defined as a failure of automatic ESF initiation signal generation. In terms of token passing protocol, it has several characteristics which is distinct from other communication networks:

- A token controls the right of access to the physical medium; the station which holds the token has momentary control over the medium.
- The token is passed by stations residing on the medium. As the token is passed from station to station a logical ring is formed.
- Steady-state operation (the network condition where a logical ring has been established and no error conditions are present) requires the sending of the token to a specific successor station as each station is finished transmitting its data frame.

The token passes the right to transmit among all stations in the logical ring. Each participating station knows the address of its predecessor (the station from which it received the token), referred to as previous station (PS). It knows its successor (which station the token should be sent to next), referred to as Next Station or NS. It knows its own address, referred to as this station (TS). These predecessor and successor addresses are dynamically determined and maintained by the algorithms described. Whenever a station changes its successor (NS), an

indication of this change is passed to the management entity. Because only one token is allowed to exist on the network, only one station can transmit at any one time, and collisions cannot occur. The general specifications of major operation process of Profibus protocol are provided in the following sections, and the corresponding hazardous states of network communication are discussed. Table 3.1 lists the identified hazardous states of the target network communication system.

3.1.1.1 Token Reception

After each station has completed transmitting any data frames it may have and has completed other maintenance functions, PS passes the token to its successor, TS which receives a token frame addressed to itself from a previous registered station. After sending the token frame, PS listens for evidence that its successor has heard the token frame and is active. If PS hears a valid frame following the token within one slot time, it assumes that TS has the token and is transmitting. Otherwise the PS attempts to assess the state of the network.

3.1.1.2 Data Transmission

When TS has data to transmit, TS acquires the token and attaches the data and control information to the token to create a data frame, which is then transmitted to the destination station on the ring. When TS receives a token frame, a service application block in the network module passes the token frame to the controller, which accepts the service request and attempts to transmit the data to the next station. The transmitted data frame circulates around the ring, and is finally removed when it reaches the intended destination station, or NS. which copies the information and send the returning frame to TS for further processing. TS can check the returning frame to see whether the frame was seen and subsequently copied by the destination station in error-free form. If the network is quiet and none of the stations has any data to transmit, the token simply circulates around the ring

continuously.

3.1.1.3 Data Reception

The station which receives the frame will re-transmit the frame to TS until it reaches the destination station and the copied data frame and is subsequently indicated to the appropriate sublayer of TS. After TS reads the data, sets the address recognised and frame copied bits in the frame status field, it transmits the frame to other next destination stations if any.

3.1.1.4 Token Passing

When the data frame has been successfully delivered to the destination station, the station must pass the token frame to the next token destination station , or NS, and completes its message cycle. In other words, a station attempts to pass the token to its successor or solicit a new successor. If the address of the successor, NS, is known, the station performs a simple token pass following any new successor solicitation. If the successor responds and the station hears a valid frame, the station has completed its token passing obligations. When a new successor is solicited by opening a response window, the station allows new stations to enter the logical ring before passing the token.

3.1.2 Identification of Hazardous States in System Level

Based on the identified hazardous states in protocol-level, the hazardous states of network failure in system-level can be identified based on top-down approach. Since the main function of ESF-CCS is to actuate ESF component by generating automatic ESF actuation signal via LCs where GCs generate and transmit LC input signal, the failure of automatic signal generation by LC in ESF-CCS for

the field component actuation in ESFAS condition can be defined as top hazardous state. This can be caused by a failure to provide input to a corresponding LC by GCs which can be categorized as:

- Failure of LC input generation by GC
 - Failure of token reception by GC
 - Failure of data transmission by GC
 - Failure of token reception by GC
- Failure of data reception by LC

To achieve diversity concept to ensure reliable ESF actuation signal generation via ESF-CCS, the redundant GCs, LCs, and network bus are implemented in ESF-CCS. In each division, there are three GCs which transmit the LC input signal based on two-out-of-four auctionnering results from four channel outputs from the PPS. The signals from GCs are processed in the LCs based on two-out-of-three voting logic. When a LC receives more than two actuation signals, it generates the control signal for the field components. In addition, there is a hot-standby backup LC which takes over the task of main LC when a malfunction or a failure of a main LC is detected. In terms of network bus, the GCs transmit the LC input signal via two redundant network buses to ensure data transmission when each bus is not functioning because of contention. Therefore, above hazardous states can be structured in detailed considering the redundant structure of GCs, LCs, and network bus in ESF-CCS as follows:

- Failure of LC input generation by GC
 - Failure of token reception by GC
 - Failure of token reception by GC 1 through network bus 1
 - Failure of token reception by GC 1 through network bus 2
 - Failure of token reception by GC 2 through network bus 1

- Failure of token reception by GC 2 through network bus 2
 - Failure of token reception by GC 3 through network bus 1
 - Failure of token reception by GC 3 through network bus 2
- Failure of data transmission by GC
 - Failure of data transmission by GC 1 through network bus 1
 - Failure of data transmission by GC 1 through network bus 2
 - Failure of data transmission by GC 2 through network bus 1
 - Failure of data transmission by GC 2 through network bus 2
 - Failure of data transmission by GC 3 through network bus 1
 - Failure of data transmission by GC 3 through network bus 2
- Failure of token passing by GC
 - Failure of token passing by GC 1 through network bus 1
 - Failure of token passing by GC 1 through network bus 2
 - Failure of token passing by GC 2 through network bus 1
 - Failure of token passing by GC 2 through network bus 2
 - Failure of token passing by GC 3 through network bus 1
 - Failure of token passing by GC 3 through network bus 2
- Failure of data reception by LC
 - Failure of data reception by LC 1a through network bus 1
 - Failure of data reception by LC 1a through network bus 2
 - Failure of data reception by LC 1b through network bus 1
 - Failure of data reception by LC 1b through network bus 2

3.2 Identification of Failure Mechanisms of Network Communication

Based on the OSI layer of Profibus protocol, the failure mechanism in one (Physical Layer), two (Data Link Layer), and seven (Application Layer) layers are identified. In terms of failure causes, soft errors in Profibus protocol, or token passing protocol can be described as either isolating or non-isolating errors [61]. An

isolating error is an error that can be traced back to a single station on the ring, and a non-isolating error is one that cannot. In other words, isolating error indicates an error condition with a particular station on the ring, thus, it can be isolated to a particular station, while non-isolating errors are usually reported by the active monitor, which is not attributed to a specific station. Isolating errors include line errors, burst errors, internal errors, and abort errors. Non-isolating errors include lost frames, congestion, token errors, and frequency errors. In this study, the isolating errors were treated as the main failure causes in the Profibus protocol.

3.2.1 Failure Mechanisms in Physical Layer

The IEC 61158-2 standard defines the Physical layer for both Profibus-DP and non-DP applications [62]. The major function of Physical layer is to receive data units from the Data Link layer and to encode them by adding communications framing information, and transmits the resulting physical signals to the transmission medium at one node. Signals are then received at one or more other nodes, and decoded by removing the communications framing information, before the data units are passed to the Data Link layer of the receiving device.

Typical networks lose or corrupt packets, disk and tape storage require re-reads of data (or even error correction), and large memory arrays may have bits corrupted by a particles. These random events occur regularly in the network systems, Under conditions that can cause these types of errors, the system's performance is determined both by the design, and by probability. Serial data communications systems, such as HR-SDL and HR-SDN network communication, must also deal with probabilistic forms of errors. The amount of error detection and recovery built into the system is often determined by the tolerance of the system to bit errors, and how often these errors occur. In these types of systems the errors are (for the most part) caused by either intrinsic or extrinsic noise sources that can affect any or all parts of a data link. The measurement and specification of a bit

error rate (BER) exists as a way to quantify the susceptibility of a digital link to these noise factors.

The Profibus-DP protocol uses coaxial cable or broadband as a transmission medium. When data are transmitted over a data link through coaxial cable, errors may be introduced into the network module as a result of noise or interference caused by external factors in the transmission medium. If errors are introduced into a token or data frame, then the integrity of the system, including the network module, may be compromised. In the case of network communication in a communications system, the transmission of the data or token frame which consists of bit error may be affected on the receiver station by transmission channel noise, interference, and distortion, among other factors [63].

3.2.2 Failure Mechanisms in Data Link Layer

The layer two (Data Link layer) of Profibus OSI model implements the functions of medium access control as well as that of logical link control, i.e. transmission and reception of the token and data frames [64]. The latter includes the data integrity function, e.g. the generation and checking of checksums.

The MAC sublayer performs several functions that are loosely coupled [60]. The descriptions and specifications of the MAC sublayer in this standard are organized in terms of one of several possible partitioning of these functions. The partitioning used here is illustrated in Figure 3.2, which shows five asynchronous logical machines where each of which handles separate MAC functions. The detailed descriptions of key features in MAC sublayer can be summarized as follows:

- Interface machine (IFM): This machine acts as an interface and buffer between the logical link control (LLC) and MAC sublayers and between network management and the MAC sublayer. It interprets all incoming data frames and other service primitives and generates appropriate outgoing

service primitives.

- Access control machine (ACM): This machine cooperates with the ACMs of all other stations on the bus in handling the token to control transmission access to the shared bus. The ACM is also responsible for initialization and maintenance of the logical ring, including the admission of new stations.
- Receive machine (RxM): This machine accepts atomic symbol inputs from the Physical layer and assembles them into frames which it validates and passes to the IFM and ACM. The RxM accomplishes this by recognizing the frame start and the frame end delimiters (SD and ED), checking the FCS and validating the frame's structure.
- Transmit machine (TxM): This machine generally accepts a frame from the ACM and transmits it, as a sequence of atomic_symbols in the proper format. The TxM builds a MAC protocol-data-unit by prefacing each frame with the required preamble and SD, and appending the frame-check sequence (FCS) and ED.

For performing fieldbus communication, above hardwares, including a processor unit for executing softwares functions for token passing protocol, are required. Therefore, the failure of hardware components in stations comprising the system must be considered as one of the failure mechanism for network communication failure because failure of hardwares and software function can result in failure of token passing protocol.

3.2.3 Failure Mechanisms in Application Layer

Layer seven (Application layer) defines the functions, services and message contents for Profibus communications. In other words, The Application layer provides user programs with a means to access the fieldbus communication environment. In

this respect, the Application layer can be viewed as a window between corresponding application programs [65]. For optimum fulfillment of the requirements of different areas of use, the functions of the Profibus-DP communication protocol are distributed over three performance levels: DP-V0, DP-V1 and DP-V2, as shown in Figure 3.1.

General Profibus DP protocol resident on a master device is composed of two fundamental applications named user-interface and direct data link mapper [66]. The user-interface represents the core of the protocol and is responsible for the correct execution of all operations foreseen by the standard, such as for instance the polling of the slaves and the interface with user applications.

The direct data link mapper has the task of mapping the requests coming from the user-interface onto FDL services. To this purpose, it is important to point out that, contrarily to what could be expected, the facilities for handling cyclic operations supplied by FDL are not used by the DP protocol for the cyclic polling of the slaves. The reason is that FDL handles the poll lists (used by the cyclic services) exclusively with low priority service requests, while, in order to ensure the complete execution of a polling cycle at each token receipt, these requests must be of high priority. Profibus DP uses two FDL services for implementing its functions: send and request data with reply (SRD) and SDN.

Since the target system uses Profibus protocol based on SDN, the failure of software functions implemented in the Application layer of each station must be considered. Failure of the Application layer can result in failure of interfacing between FDL services in layer two, thus, a station fails to receive or transmit the token or data frame.

3.3 Quantification of Network Failure Mechanisms

In summary, the functions specified in the Profibus protocol are performed by hardware components and software functions in network modules of the GCs and

LCs in the ESF-CCS. Either failure of the hardware components of the network module or failure of the software to perform the intended function may cause network communication failure, thereby resulting in a failure to generate ESF actuation signal in ESFAS condition. In addition, electromagnetic interference or other environmental interference in the medium may cause bit errors or faults in a token or data frame and result in such a failure. To estimate the risk effects of network communication failure between the GCs and LCs on ESF-CCS signal failure in a certain ESF initiation condition, a quantification scheme for each identified cause of failure is proposed.

3.3.1 Quantification of Hardware Failure Probability

Both HR-SDN and HR-SDL systems are adopted for the network communication between the GCs and LCs. These systems is based on a safety-grade PLCs [8]. The PLC consists of various modules such as a power module, a processor module, communication modules, digital input/output modules, analog input/output modules [66]. The PLC installs two independent power modules in a rack. The power module has a 100% power supply capability for each. Accordingly, even when there is a fault in one power module, it does not affect the PLC operation. The processor module uses a Texas Instrument DSP and the real-time operating system named pCOS2 was developed based on the Micro-C real-time operation system. processor module consist of a single or redundant [67]. The PLC can extend the number of input/output module through a local bus extension module.

The communication modules implemented in safety-graded PLC consist of Profibus-Fieldbus Message Specification (FMS), HR-SDL, and HR-SDN. Physical layer mediums are supplied both RS-485 for electrical communication and Optical communication. HR-SDL module were developed based on the RS-232C. The Digital Input and Output modules consist of 24VDC, 48VDC, 120VAC and 230VAC digital input and 24VDC, 48VDC 125VDC, Relay, Solid State Relay digital output module.

The Analog Input and Output modules consist of voltage and current input and output module, resistance temperature detector module and thermocouple module.

Based on PLC module data, the failure rates of the hardware components, with the exception of the network modules, were estimated based on the number of modules in each type of controller, as shown in Table 3.2 [68].

In terms of HR-SDL and HR-SDN network modules in PLC, the failure probability of hardware components in each network module were derived considering the different features of communication modules.

For HR-SDL communication module, hardware of the HR-SDL communication module consists of a CPB (NCPB-1Q) and a driver board (NDRVOM-4Q) as shown in Figure 3.2 [69]. The CPB consists of dual port memory (DPM), central processor unit (CPU), read-only memory (ROM) and random access memory (RAM), and exchanges data with processor module through DPM-CPB. The Driver Board (DRB) consists of DPM, EC1 and ROM, and exchanges data with the CPB through DPM-DRB. The micro processor in the CPB is SMQ 320C32 PCMM-60M CPU, and the CPB uses 32KWords Dual Port Memory, 512KW Flash Memory, and 512KW SRAM. Since the data transfer between the CPB and the processor module is achieved through a dual port memory without interrupt, the safety function of the processor module is performed separately from communication module. The DRB sends/receives data to/from other PLCs through EC1 separately from the CPB. The failure probability for hardware components, including network module, network driver module, fiber optic transmitter, and receiver, are derived based on the module-level failure rate. Table 3.3 shows the failure rate of each module in HR-SDL network communication module [70].

In case of HR-SDN network communication module, its sub-level hardware components, including the transmitter, the receiver, and other hardware modules, must be considered. In this study, the failure rates for various hardware components

specified in the block diagram of the Profibus-DP controller, as shown in Figure 3.3, including those for the microprocessor, the interrupt controller, the serial interface, the ASIC, and the RAM, were considered [57]. The failure probability for each hardware component was determined based on a reliability model for a digital feedwater control system [71]. Regarding the transmitter and receiver in the serial interface, the average failure rate for the photonic component was estimated based on the reliability data of photonic components and their subsystems [72]. Table 3.4 shows the failure rates for sub-level hardware components in the network module of Profibus-DP controller.

To estimate the probability of hardware failure, the mean unavailability of the components of a network module must be considered based on the case of a general electric component that undergoes periodic inspection at specified intervals. The mean unavailability (Q_{ave}), or the time-dependent probability for a random failure, of a component with a constant failure rate of can be calculated as one-half of the product of the failure rate (λ_0) and the periodic test interval (T), as shown in Equation (1) [73].

$$Q_{ave} = \frac{1}{T} \int_0^T Q(t) dt = 1 - \frac{1}{\lambda_0 T} (1 - e^{-\lambda_0 T}) \simeq \frac{1}{2} \lambda_0 T \quad (1)$$

In this study, two periodic test intervals for the hardware components in the network modules of the GCs and LCs were considered. The components in the network modules were assumed to be manually tested once per month and to undergo automatic periodic testing by the self-diagnostic function implemented in the PLC. General PLC operations include a self-diagnostic process or the PLC scan process, which enables internal diagnostics and communication task tests to be performed by the CPU [74]. In general, the PLC scan is dependent on the complexity of the software program implemented in the PLC and the processing capability of the processor in the PLC. Figure 3.4 and 3.5 shows the block diagram

of the PLC and the general scan process for the PLC, respectively. Generally, the PLC scan time ranges from a few milliseconds to one-hundred milliseconds.

In this study, the interval of the automatic tests performed by the PLC self-diagnostics for the network module hardware components was assumed to be 50 milliseconds. Because the functions of the GCs and LCs are based on repetitive network communication with fixed sets of transmitted data, all design-intended functions of the GCs and LCs were assumed to be tested in every PLC self-diagnostic cycle; thus, the coverage of the automatic test was assumed to be unity.

3.3.2 Quantification of Software Failure Probability

Because software, unlike hardware, does not fail, break, or wear out over time, equivalent accelerated stress testing cannot be performed on software [31]. In principle, software takes inputs from other systems and produces outputs that are used either by humans or by other software and hardware. Regarding the software failure probability quantification method, a qualitative approach was suggested which considers the complexity of the application function and the level of the verification and validation (V&V) process required for application software in a NPP [75]. In the proposed quantification method, indirect evidence can be applied to estimate the failure probabilities of application software modules using the metrics of complexity and V&V level, for which the safety integrity level (SIL) is used as an estimator of the V&V process, as shown in Table 3.5.

Because the GCs and LCs in the ESF-CCS also undergo a thorough V&V process for implementation in an NPP, the failure probability of the software implemented in the GCs and LCs can be similarly treated using this approach. With regard to the SIL class, the frequency of error occurrence in the GC and LC software can be considered to be infrequent, and the consequence of software failure can be considered to be critical because the software performs the function of

transmitting safety-critical information and the ESF actuation signal can be generated by CIM via manual actuation even if when automatic signal generation is not available through ESF-CCS. Table 3.6 and Table 3.7 shows the definition used for risk-based software integrity level scheme for consequence and likelihood of occurrence used in the proposed qualitative approach [76]. Therefore, the software failure probability of network module in GC and LC were assumed as $1.0\text{E-}04$ and that of Application layer in GC and LC were assumed as $1.0\text{E-}03$ based on Tables 3.5 and 3.8, in this study.

3.3.3 Quantification of Failure Probability related to Bit Error

Safety-critical instrumentation generally falls into one of two operation modes which is continuous and low demand mode [75]. The safety-critical I&C system in NPP is operated as low demand mode since its safe operation is called upon at the time point of demand when NPP is at abnormal state. Therefore, the probability of the introduction of error in the transmitted data in ESF actuation condition can be treated as the probability of failure on demand (PFD). In addition, a single bit error in a token frame or data frame that is transmitted between the GCs and LCs in the ESF-CCS was assumed to have a critical effect on the network communication, thus resulting in on-demand failure of network communication.

In terms of the probability of the introduction of error into the system, the BER is a key parameter that is used to assess systems that transmit digital data between locations. Generally, systems for which the BER is applicable include fiber-optic data systems and other systems, such as Profibus network systems, that transmit data over a transmission medium in which noise and interference may cause degradation of the digital signal. BER is defined as the ratio of the number of bits received incorrectly, compared to the total number of bits transmitted as shown in Equation (2).

$$BER = \frac{\text{Expected number of erroneous bits}}{\text{Total number of sent bits}} \quad (2)$$

As shown in Table 3.9, the bit error probability values of transmission systems for bus drivers and serial links is in the range from 1.00E-06 to 1.00E-12 [77]. In the Profibus network, Physical layer implementation is generally specified for three types, and each type exhibits particular signaling rates and transmission characteristics as follows. Note that the BER of each Physical layer implementation is generally on the order of 1.0E-08 [78].

- Fiber optic media: 1 Mbps; BER = 10⁻⁹~10⁻⁸
- Phase-continuous-FSK: 1, 5, 10 Mbps; BER = 10⁻⁹~10⁻⁸
- Phase-coherent-FSK: 5, 10 Mbps; BER = 10⁻⁹~10⁻⁸

In this study, the estimated expected number of erroneous bits in each frame was treated as the probability of token frame or data frame corruption caused by bit errors introduced by the bus medium, which depends on the length of the token frames and the data frames in the Profibus-DP protocol, as shown in Figure 3.6 and Table 3.10 [79]. Note that the bit error detection measures were not considered since the coverage of these error recovery operations for network failure in ESF-CCS has not yet been investigated.

Table 3.1 Major operation processes of token bus protocol and corresponding hazardous states for GC and LC in ESF-CCS

Major Operation Process	Description	Hazardous States
Token frame reception	A station receives a token frame addressed to itself from a previous registered station	Failure of token reception by GC
Data frame transmission	A station accepts the service request and transmits the data to the next station	Failure of data transmission by GC
Data frame reception	If the frame's destination address matches the station address, the data frame is indicated to the sublayer of the station	Failure of data reception by LC
Token frame passing	If the data frame is delivered to the next station, the station passes the token frame to the next token destination station	Failure of token transmission by GC

Table 3.2 Failure rate of various modules in a single GC and LC

Component	Module	Quantity	Failure rate/module (/hr)
GC	Power supply	2	2.15E-05
	Processor	1	7.75E-06
	Digital input	4	6.25E-06
	Base board	1	0.98E-06
LC	Power supply	2	2.15E-05
	Processor	2	7.75E-06
	Analog input	1	4.06E-06
	Analog output	1	4.06E-06
	Digital input	2	6.25E-06
	Digital output	2	5.93E-06
	Base board	2	0.98E-06

Table 3.3 Module-level failure rate of HR-SDL communication module

Module	Failure rate/module (/hr)
Processor module (NCPU-1Q)	1.26E-05
Network module (NCPB-1Q)	4.85E-06
Network driver module (NDRVOM-4Q)	7.99E-06
Fiber optic Transmitter (NDA8-1Q)	7.82E-06
Fiber optic Receiver (NAD8-1Q)	3.51E-06

Table 3.4 Failure rates for sub-level hardware components in the network module of Profibus-DP controller

Sub-level component in the network module		Failure rate (/hr)
Network interface module	Microprocessor	3.30E-08
	Interrupt controller	1.60E-09
	Clock reference failure	5.20E-07
	ASIC	4.60E-07
	RAM	3.30E-07
Transmitter		1.45E-06
Receiver		2.94E-06

Table 3.5 Software integrity levels and their corresponding reliability targets from IEC 61508

Software Integrity Level	Probability of a failure on demand (PFD) of the safety function
1	$10^{-2} \leq PFD \leq 10^{-1}$
2	$10^{-3} \leq PFD \leq 10^{-2}$
3	$10^{-4} \leq PFD \leq 10^{-3}$
4	$10^{-5} \leq PFD \leq 10^{-4}$

Table 3.6 Definition of consequences described in IEEE Std 1012-2004 regarding software integrity levels

Consequence	Definition
Catastrophic	Complete mission failure, loss of system security and safety.
Critical	Partial loss of mission, major system damage.
Marginal	Severe injury or illness, degradation of secondary mission, or some financial or social loss.
Negligible	Minor injury or illness, minor impact on system performance, or operator inconvenience.

Table 3.7 Categories of likelihood of occurrence described in IEEE Std 1012-2004 regarding software integrity levels

Category	Definition
Reasonable	Many times in system lifetime
Probable	Several times in system lifetime
Occasional	Once in system lifetime
Infrequent	Unlikely in system lifetime

Table 3.8 Assignment of software integrity levels based on IEEE Std 1012-2004

Description	Software integrity level
-Software element must execute correctly or grave consequences (loss of life, loss of system, economic or social loss) will occur. -No mitigation is possible.	4
-Software element must execute correctly or the intended use (mission) of the system/software will not be realized, causing serious consequences (permanent injury, major system degradation, economic or social impact). -Partial to complete mitigation is possible.	3
-Software element must execute correctly or an intended function will not be realized, causing minor consequences. -Complete mitigation possible.	2
-Software element must execute correctly or intended function will not be realized, causing negligible consequences. -Mitigation not required.	1

Table 3.9 Typical bit error probability values for various transmission systems

Bit error probability	Transmission system
$> 1.00\text{E-}03$	Radio link
$1.00\text{E-}04$	Unshielded telephone cable
$1.00\text{E-}05$	shielded, "twisted-pair" telephone cable
$1.00\text{E-}06 \sim 1.00\text{E-}07$	Digital telephone cable of Deutsche Telecom (ISDN)
$1.00\text{E-}09$	Coaxial cable in locally delimited applications

Table 3.10 Description of the data in data frame of network communication between a single GC and LC

Source	Destination	Signal	Type	Number of signal	Range
GC	LC	Operational signal	BOOL	11	0 or 1
GC	LC	Testing condition	BOOL	11	0 or 1
GC	LC	Heartbeat of GC	INTEGER	1	3000 ~ 3255 4000 ~ 4255 5000 ~ 5255

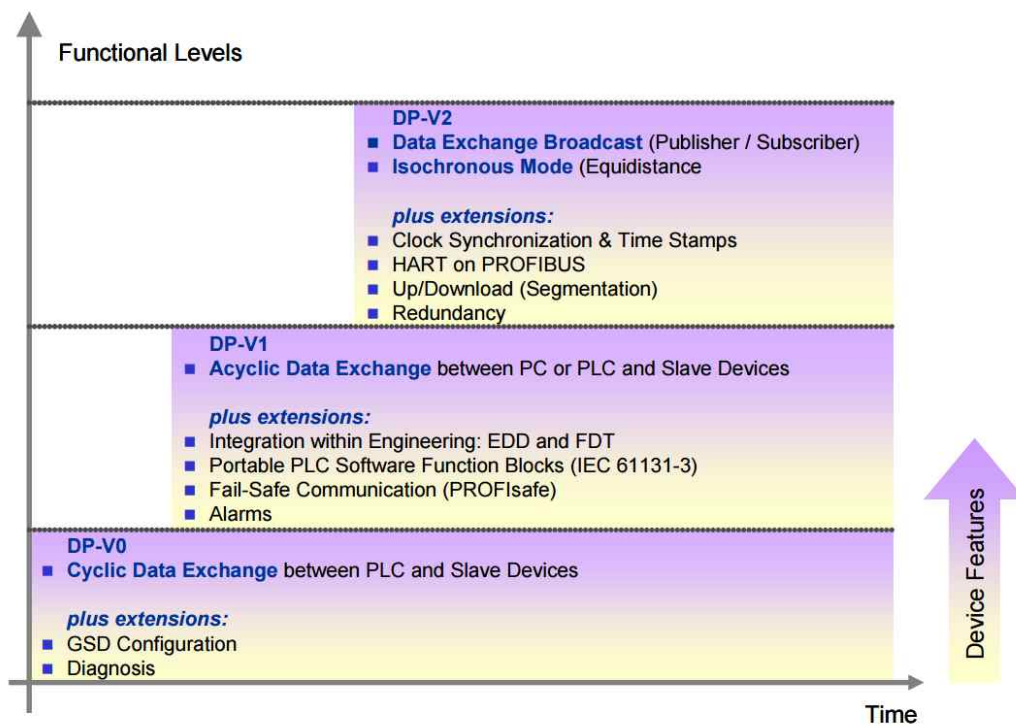


Figure 3.1 An example of various service levels of Profibus-DP protocol

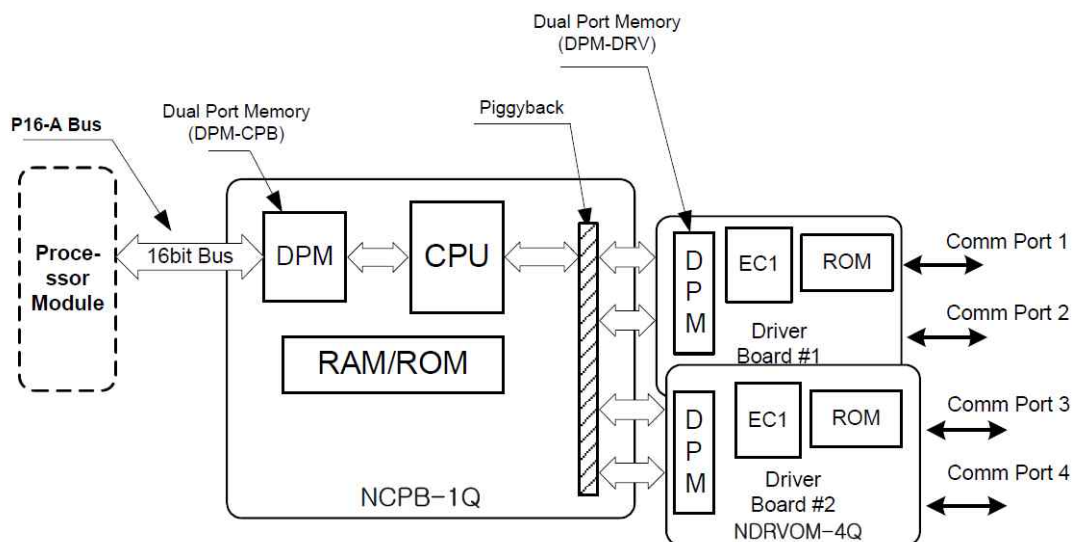


Figure 3.2 Hardware structure of HR-SDL communication module

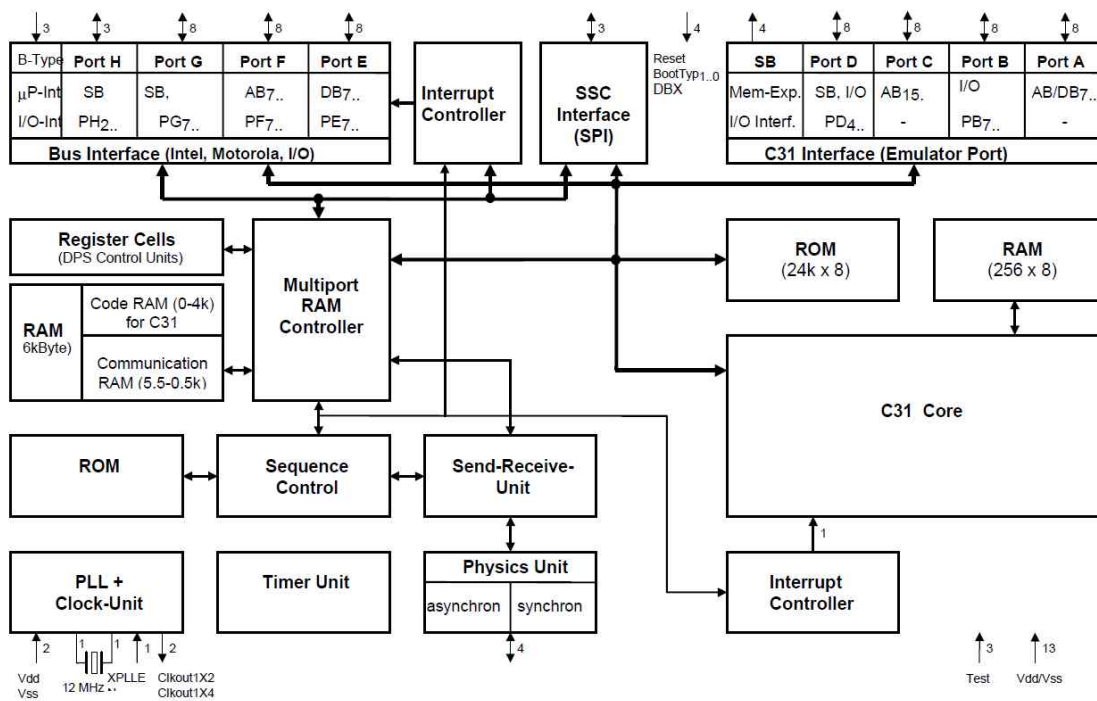


Figure 3.3 Block Diagram DPC31 (Siemens Profibus-DP Controller)

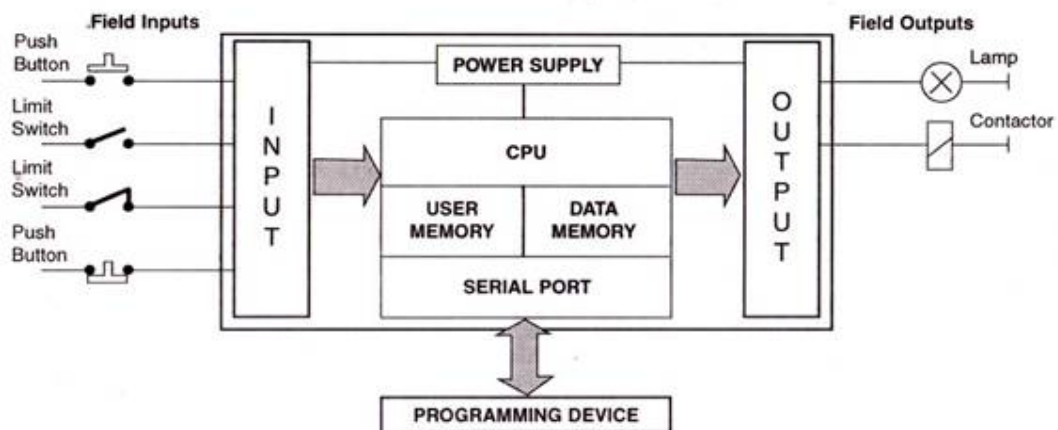


Figure 3.4 Block diagram of general programmable logic controller

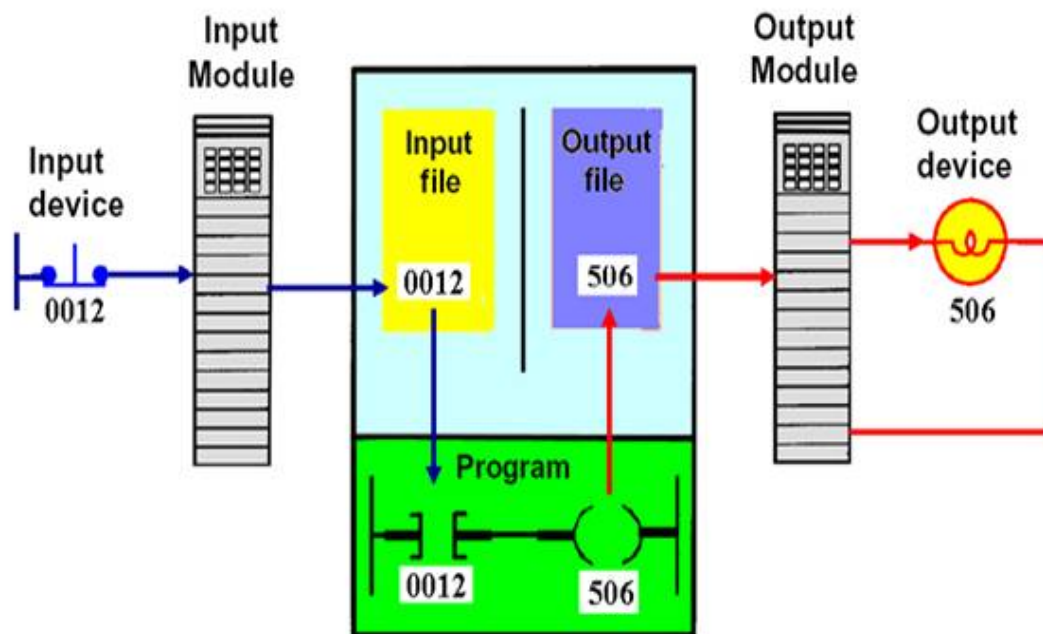


Figure 3.5 Description of scan process of general programmable logic controller

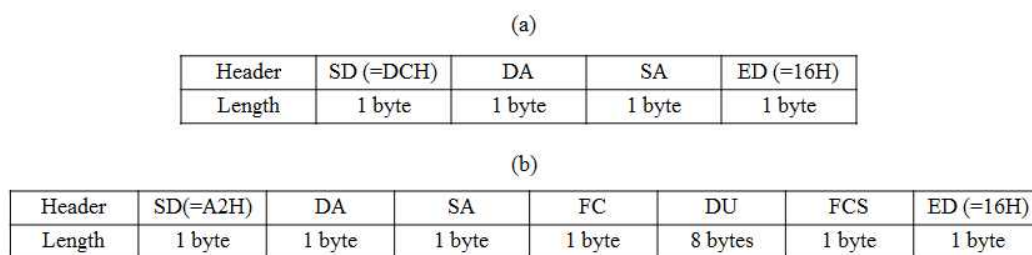


Figure 3.6 Profibus-DP protocol frame structure: (a) token frame format, (b) data frame format with fixed lengths of the data units

Chapter 4. Development of fault-tree model of network communication

4.1 Analysis on the Signal Flow in ESF-CCS

The digital ESF-CCS is an extension of the PPS and is used for interfacing between the PPS cabinet and various field components, such as pumps and valves, comprising the ESFs. The function of ESF-CCS is to provide initiating signals for ESF components that require automatic actuation when the abnormal conditions in a NPP are detected and when mitigating the design-basis or loss-of-coolant accident. It is notable that the ESF-CCS of the APR-1400 plays the roles of both the ESFAS and the plant control system of the Optimized Power Reactor-1000 (OPR-1000). Assuming that the ESF of the APR-1400 is the same as that of the OPR-1000, the ESF-CCS provides an initiation signal to each of the following independent ESF functions such as SIAS, CIAS, CSAS, RAS, MSIS, and AFAS. Especially, SIAS, CSAS, RAS, AFAS are used in various mitigation actions in case of design-basis or loss-of-coolant accident (LOCA). Table 4.1 shows various mitigation actions based on OPR-1000 PSA model and their required ESF actuation signals. Detailed description of the mitigation action and required field component actuation are discussed in the following sections.

4.1.1 Required ESF signals for Accident Mitigation Actions

4.1.1.1 High Pressure Safety Injection System

The high pressure safety injection system (HPSIS) is part of the emergency core cooling system (ECCS) that performs emergency coolant injection and recirculation functions to maintain reactor core coolant inventory and adequate decay

heat removal following a LOCA [80]. The coolant injection function is performed during a relatively short-term period after LOCA initiation. During a normal operation of a NPP, HPSIS is in a standby mode. When SIAS is generated by ESF-CCS, HPSIS automatically enters to injection mode; HPSI pumps are automatically operated and the HPSI header isolation motor-operated valves (MOVs), which isolates HPSIS from cold leg in a standby mode, are opened, thus, the borated water from refueling water tank (RWT) is injected to the reactor coolant system (RCS). Figure 4.1 shows the arrangement of HPSIS system in a injection mode. After high pressure injection, a recirculation mode of operation to maintain long-term, post-LOCA core cooling are followed. If the water level is below 5% of the design basis, RAS is generated; the containment sump isolation MOVs are opened to switch the water source from the RWT to containment sump. Figure 4.2 shows the arrangement of HPSIS system in a recirculation mode.

In case of the mitigation action which requires both safety injection and recirculation cooling of the RCS via HPSIS, related ESF signals include SIAS and RAS, and the actuated ESF components include HPSI pumps, HPSI header isolation valves, and CS isolation MOVs.

4.1.1.2 Low Pressure Safety Injection System

The low pressure injection system, or residual heat removal system, is designed to inject water from the refueling water storage tank into the reactor coolant system during large breaks, which would cause a very low reactor coolant system pressure [81]. When SIAS is generated, LPSIS automatically enters to an injection mode; LPSI pumps are operated and each LPSI header isolation MOV, which prevents the counterflow from the RCS to LPSIS in a standby mode, is opened. The borated water in the RWT is then injected to the RCS where the pressure of the RCS is below certain level. Figure 4.3 shows the arrangement of LPSIS in an injection mode.

In case of the mitigation action which requires the safety injection of the RCS via LPSIS, related ESF signals include SIAS, and the actuated ESF components include LPSI pumps, and LPSI header isolation valves.

4.1.1.3 Auxiliary Feedwater System

The auxiliary feedwater (AFW) system's principal role is to support removal of stored and decay heat from the RCS [82]. The steam generators (SGs) act as a heat sink during both normal operation and following reactor trips. During normal operation, the main feedwater system provides feedwater to the SGs, where it is converted to steam and then used to drive the main turbine and provide process steam for various plant equipment. During normal power operation, the AFW system is in standby.

Although AFW system can be used in support of normal plant startup and shutdown, it is specifically designed for the mitigation of the consequences of design basis transients and accidents, including loss of main feedwater (LOFW), main feed line break (MFLB), main steam line break (MSLB), small- and large-break LOCA, SG tube rupture, and others. Following an operating transient or accident, the AFW system is used to provide a safety-related source of water to the SGs. When main feedwater system is not available, the water, which is delivered by the AFW system, is heated and vaporized in the SGs. To deliver sufficient AFW, AFW motor-driven pumps (MDPs) and AFW turbine-driven pumps (TDPs) are used. In addition, AFW isolation MOVs are opened to deliver the water source from condensate storage tank (CST) to the SGs. Steam generated then can be released to the atmosphere through the safety-related main steam safety valves or atmospheric dump valves or to the atmosphere and/or condenser through nonsafety-related steam dump valves. Figure 4.4 shows the arrangement of the AFW system in an operational mode.

In case of the mitigation action which requires the auxiliary feedwater deliver to the SGs via AFW system, related ESF signals include AFAS, and the actuated

ESF components include Auxiliary Feedwater MDPs, Auxiliary Feedwater TDPs, and Auxiliary Feedwater Isolation MOVs.

4.1.1.4 Containment Spray System

Upon the occurrence of either a secondary break or primary break inside the containment building, the containment atmosphere would become filled with steam. To reduce the pressure and temperature of the building, the containment spray system is automatically started. The containment spray (CS) pump will take a suction from the refueling water storage tank and pump the water into spray rings located in the upper part of the containment [83]. The water droplets, being cooler than the steam, will remove heat from the steam, which will cause the steam to condense. This will cause a reduction in the pressure of the building and will also reduce the temperature of the containment atmosphere (similar to the operation of the pressurizer).

When CSAS is generated, CS pump is operated and CS pump header isolation valve is opened to inject the water inside the containment. Figure 4.5 shows the arrangement of the CS system in a injection mode. To control the chemical condition in the system, high concentration of hydrazine is mixed with the borated water in the RWT and it is used as a water source to reduce the temperature inside containment building. To ensure sufficient heat removal via CS, CS pump sprays the water after it passes through CS heat exchanger.

Like the residual heat removal system, the containment spray system has the capability to take water from the containment sump if the refueling water storage tank goes empty. Figure 4.6 shows the arrangement of the CS system in a recirculation mode. When the water level of RWT decreases below 10% from the design basis, RAS is generated and the water source of CS pump changes to containment sump. The containment sump isolation MOVs are opened by RAS and CS pumps take a suction from the containment sump and pump the water into spray

rings to condense the steam into liquid in the containment.

In case of the mitigation action which requires recirculation cooling of the containment via CS system, related ESF signals include CSAS and RAS, and the actuated ESF components include CS pumps, CS header isolation valves, CS heat exchangers, and CS isolation MOVs.

4.1.2 Functional Allocation of ESF Components in ESF-CCS

The safety related components in NPPs are traditionally controlled by single-LCs. Traditional single-LC systems utilize dedicated processors for each component but that components independence is compromised through a sharing of power supplies, auxiliary logic modules and auxiliary I/O cards. Since components are assigned to ESF-CCS functional groups in a manner consistent with their process relationship, the key issues for the design of multi-LC was addressed to allocate the components to the each multi-LC through plant and function analysis and grouping [68, 84].

In terms of the functional allocation of the LCs in the ESF-CCS, the system is composed of approximately 300 components related to various safety actuation signals provided by the ESF-CCS, including the safety injection actuation signal (SIAS) and the containment spray actuation signal (CSAS) [85]. All safety injection components are functionally allocated in the four safety-related divisions; approximately 110 components are equally divided among the four divisions. In each division of the ESF-CCS, the safety functions are also functionally allocated in each LC. In this study, the assumptions on the LC allocation to the field components are adopted from the previous study [20]; that is, same LC module is assumed to be used for the ESF components which is allocated to the same number of K-relay output. Table 4.2 shows the detailed description of the LC modules allocated to the ESF components with the corresponding number of K-relay output.

4.2 Fault-tree Modeling of Network Communication in ESF-CCS

A fault-tree model of GC-LC network communication failure was developed based on the RM-ESFCCS, which was originally developed by Kang et al. [20] based on the redundancy concept as well as the identified hazardous states and corresponding causes of failure regarding network communication between GCs and LCs. Based on the potential hazardous states and the corresponding causes of failure that may cause a failure of network communication in the Profibus protocol, the fault-tree model of network failure in the GCs and LCs is modeled using the Advanced Information Management System for Probabilistic Safety Assessment (AIMS-PSA), which is an integrated safety assessment software package. As shown in Table 4.2, which describes required ESF component for various mitigation actions in NPP design basis accidents (DBAs), fault-tree models of a total of 36 ESFAS required safety components were developed.

Besides of the automatic ESF actuation signal generation by ESF-CCS, the human operator could also manually actuate the field components as a backup of an automated system via CIM. In addition, the DPS is an independent and separate automatic system for signal generation. Independent and dedicated sensors provide input to the DPS. DMA provides a redundant mean for the operator in the main control room to access the field components via the hard-wired path. In this study, the failure of human operator action is also modeled in the fault-tree; the failure probability of the human operator for manual actuation of ESF signal generation via DPS was assumed as 0.05 and that of the field component via CIM is assumed as 0.1 based on the conventional human error probability (HEP) method [20].

4.2.1 Fault-tree Modeling of HR-SDL Network Communication

Figure 4.7 shows the logic of a developed model for ESF-CCS signal failure for V675 in RAS condition for the ESF-CCS system applied with HR-SDL network

communication. It is notable that other ESF components can be modeled in a same manner. Since the human operator could also manually actuate the field components as a backup of PPS via CIM, the failure of remote manual actuation of specific ESF component by operator and the failure of mechanical switches are modeled. In addition, the failure of digital output (DO) module of allocated LC was modeled because the ESF actuation signal generated by LC is transmitted to individual field component by DO of LC.

In terms of signal failure for field component due to LC signal processing, both independent failure and CCF of LC hardware components (i.e. power supply, digital input, digital output, processor, base board) may cause a failure of LC signal processing. The failure of heartbeat algorithm, which is responsible for allowing backup LC to generate ESF component actuation signal when main LC is failed to function, is also considered, as shown in Figure 4.8. In addition, the ESF actuation signal failure can be caused by a failure to provide input to the corresponding LCs, including both the main LC (e.g. LC A4A) and the hot standby backup LC (e.g. LC A4B). Each logic of the failure to provide input to LCs includes the failure of network communication between GCs and corresponding LCs and failure of LC input signal generation by GCs in same division, as shown in Figure 4.9 and 4.10.

When evaluating the possibility of network failure in the LC, both the failure of the network modules required for HR-SDL communication (i.e. processor module, network module, network driver module) and the failure of the network communication protocol should be considered, as shown in Figure 4.11 and 4.12. Figure 4.13 ~ 4.16 shows the logics of failure of data reception by both main and backup LC through two redundant network buses (i.e. network bus A1 and network bus A2). Since LCs receive the data frame including ESF component actuation signal, transmitted from GCs in the same division, a failure of network communication protocol include both failure of fiber-optic receiver in LC network module and on-demand software failure of LC network module. Because redundant

bus structure is implemented in ESF-CCS, network-medium-related bit errors in the receipt of data frames from three redundant GCs via two network buses must be considered.

In addition, the failure to provide input to LCs can be caused by the failure of input processing by GCs, as shown in Figure 4.17 and 4.18. The GCs' signals are processed in the LCs based on two-out-of-three voting logic. When a LC receives more than two actuation signals, it generates the control signal for the field components in consideration of the characteristics of each component. In each GC, failure of input processing for LCs can be caused by the failure of GC hardware modules (i.e. power supply, digital input, processor, base board) and the network communication failure. The failure of GC hardware modules include independent failure and CCF of GC hardware module, and the failure of heartbeat algorithm, which is responsible for allowing LCs to generate ESF component actuation signal with alternative one-out-of-two voting logic when single GC in the same division is failed to function, as shown in Figure 4.19. In terms of network failure in each GC, both the failure of network modules in GC (i.e. processor module, network module, network driver module) and network protocol failure are considered. Based on the identified hazardous states of GC, failure of network protocol can be categorized as token reception failure, data transmission failure, and token passing failure. In case of data transmission and token passing, the failure of transmitter in GC, which are used to transmit the data and token, and failure of network module software are considered. In terms of token reception, token frame is passed from one GC station and received by other GC stations, thus, the failure of receiver in GC and the failure of network module software are considered. During the network communication by GC, token and data frames are received or transmitted via network bus; therefore, the network-medium-related bit errors in the receipt of token or data frames from different GCs via two network buses must be considered. The detailed logics of network module failure in GC and network protocol failure of

each GC through two redundant network buses are shown in Figure 4.20 ~ 4.25.

To model the failure of multiple identical components in the network interface, transmitter and receiver module as a result of shared causes, the common-cause failure (CCF) of the network modules in the main and backup LCs, and three redundant GCs must be considered. Since the main and backup LCs or three redundant GCs use same hardware module and implemented software respectively, the CCFs of both hardware and software are considered, as shown in Figure . In this study, it assumed that the failure cause of more than two modules resulted in the CCF of all the same-function modules similarly to the beta (β) factor method [86]. The β factor method is an approximation method used for the quantitative evaluation of CCFs. In this method, the likelihood of the CCF is evaluated in relation to the random failure rate for the component. A β factor is estimated such that $\beta\%$ of the failure rate is attributed to the CCF and $(1-\beta)\%$ to the random failure rate of the component. In other words, the mean availability for a CCF involving 'k' basic events Q_k is:

$$\begin{aligned} Q_k &= (1-\beta)Q_{tot} && \text{for } k=1 \\ Q_k &= 0 && \text{for } 1 < k < N \\ Q_k &= \beta Q_{tot} && \text{for } k=N \end{aligned} \quad (3)$$

Quantification of these beta factors using hard data or analytical methods is difficult since simultaneous hardware or OS failure in independent safety-graded PLCs is rare, and not observed in the field data. Therefore, assignment of beta factor values require the use of expert judgment, based on a qualitative assessment of the similarities between the functions. The recommended beta factor is between 0.1 and 0.001 depending on the similarity of the functions [87, 88].

4.2.2 Fault-tree Modeling of HR-SDN Network Communication

Figure 4.26 shows the logic of a developed model for ESF-CCS signal

failure for V675 in RAS condition for the ESF-CCS system applied with HR-SDN network communication. It is notable that the developed logic is modeled in a same manner as a developed model of ESF-CCS signal failure for HR-SDL network communication due to a same system configuration. A failure of network communication between the GCs and LCs may cause a failure to provide input to both the main LC and the hot standby backup LC. However, different failure logics, including the failure of network module and software failure, are considered.

In terms of network module failure, the failure of the sub-level hardware components in LC network module (i.e. microprocessors, interrupt controller, clock reference, ASIC, RAM) are considered. Figure 4.27 and 4.28 shows the logic of hardware failure of main LC and backup LC, respectively. For network module failure in GCs, the failure of microprocessors, interrupt controller, clock reference, ASIC, RAM in GCs are considered. Figure 4.29 ~ 4.31 shows the logic of hardware failure of three redundant GCs (i.e. GC A1, GC A2, GC A3), respectively.

In addition to the software failure of network modules in the allocated LC and GCs, on-demand failure of application software should be considered since HR-SDN network communication is based on Profibus-DP protocol; thus, it uses additional Application layer for cyclic communication through bus topology along with bus start up and bus diagnostic functions. Therefore, different network receiver and transmitter components compared to HR-SDL network communication are used for Profibus-DP communication. Figure 4.32 ~ 4.35 shows the logic of a failure of network protocol, especially data reception failure, by main and backup LCs through two redundant network buses. The logics of a failure of network failure, including token reception, token transmission, and data transmission, in a single GC are shown in Figure 4.36 ~ 4.38. Note that the network protocol failure of other GCs (i.e. GC A2 and GC A3) can be modeled in a same manner as GC A1.

Table 4.1 Mitigation actions regarding initiating events for OPR1000 and their required ESF actuation signals

Mitigation Action	Required ESF signal	Required Field Component Actuation
HPSIS Injection	SIAS	HPSI Header Isolation MOV
		HPSI Pump
LPSIS Injection	SIAS	LPSI Header Isolation MOV
		LPSI Pump
Auxiliary Feedwater Deliver	AFWS	Auxiliary Feedwater Isolation MOV
		Auxiliary Feedwater MDP
		Auxiliary Feedwater TDP
HPSIS Recirculation	SIAS	HPSI Header Isolation MOV
	RAS	HPSI Pump
LPSIS Recirculation	SIAS	Containment Sump Isolation MOV
		LPSI Header Isolation MOV
Recirculation Cooling	CSAS	LPSI Pump
		Containment Spray Pump
	RAS	Containment Spray Header Isolation Valve
		Containment Spray Heat Exchanger
		Containment Sump Isolation MOV

Table 4.2 Description of ESF components and corresponding LC allocation

ESFAS	Required ESF component actuation	Description	K-relay output	LC allocation
AFAS-1A	MP01A	AF pump AF-PP01A	K402A	LC A1
	V35	Modulating v/v AF-V035	K402A	LC A1
	V43	AF isol. v/v AF-V043	K402A	LC A1
	V36	Modulating v/v AF-V036	K113A	LC A2
AFAS-1B	TP01B	AF turbine (TA01B)	K402B	LC B1
	V44	AF isol. v/v AF-V044	K402B	LC B1
AFAS-2A	TP02A	AF turbine (TA01A)	K112A	LC C1
	V38	Modulating v/v AF-V038	K112A	LC C1
	V46	AF isol. v/v AF-V046	K112A	LC C1
	V37	Modulating v/v AF-V037	K413A	LC C2
AFAS-2B	MP02B	AF pump AF-PP02B	K112B	LC D1
	V45	AF isol. v/v AF-V045	K112B	LC D1
CSAS-A	PP01A	CS pump CS-PP01A	K111A	LC A3
	CSV35	Spray isol. v/v CS-V035	K304A	LC C3
CSAS-B	PP01B	CS pump CS-PP01B	K111B	LC B3
	CSV36	Spray isol. v/v CS-V036	K304B	LC D3
RAS-A	V675	CIV SI-V675	K104A	LC A4
	HX1A	Spray Hx. A inlet isol. v/v CC-V141	K114A	LC C4
RAS-B	V676	CIV SI-V676	K104B	LC B4
	HX1B	Spray Hx. A inlet isol. v/v CC-V142	K114B	LC D4
SIAS-A	HP02A	HPSI pump SI-PP02A	K109A	LC A5
	LP01A	LPSI pump SI-PP01A	K110A	LC A6
	V637	Isol. v/v SI- V637	K302A	LC C5
	V635	Isol. v/v SI-V635	K302A	LC C5
	V647	Isol. v/v SI- V647	K301A	LC C6
	V645	Isol. v/v SI-V645	K301A	LC C6
	V617	HPSI header isol. v/v SI-V617	K403A	LC C7
	V627	HPSI header isol. v/v SI-V627	K401A	LC C8
SIAS-B	HP02B	HPSI P/P SI-PP02B	K109B	LC B5
	LP01B	LPSI P/P SI-PP01B	K110B	LC B6
	V626	Iso V/V SI- V626	K302B	LC D5
	V615	Iso V/V SI-V615	K302B	LC D5
	V616	Iso V/V SI-V616	K301B	LC D6
	V625	Iso V/V SI-V625	K301B	LC D6
	V646	HPSI HDR Iso V/V SI-V646	K403B	LC D7
	V636	HPSI HDR Iso V/V SI-V636	K401B	LC D8

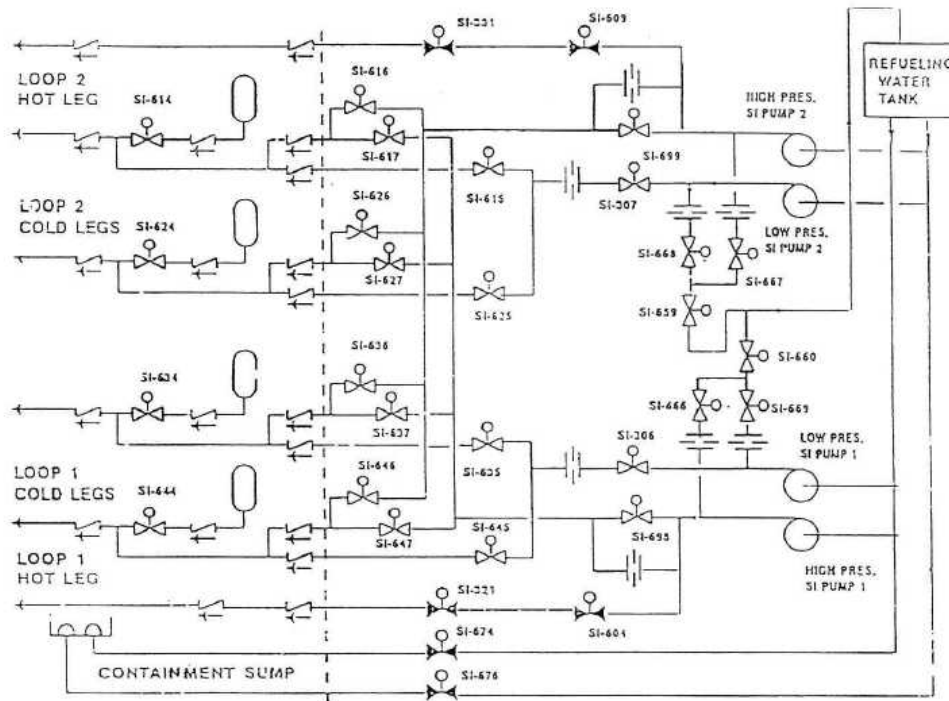


Figure 4.1 Alignment of ESF components of HPSIS in an injection mode

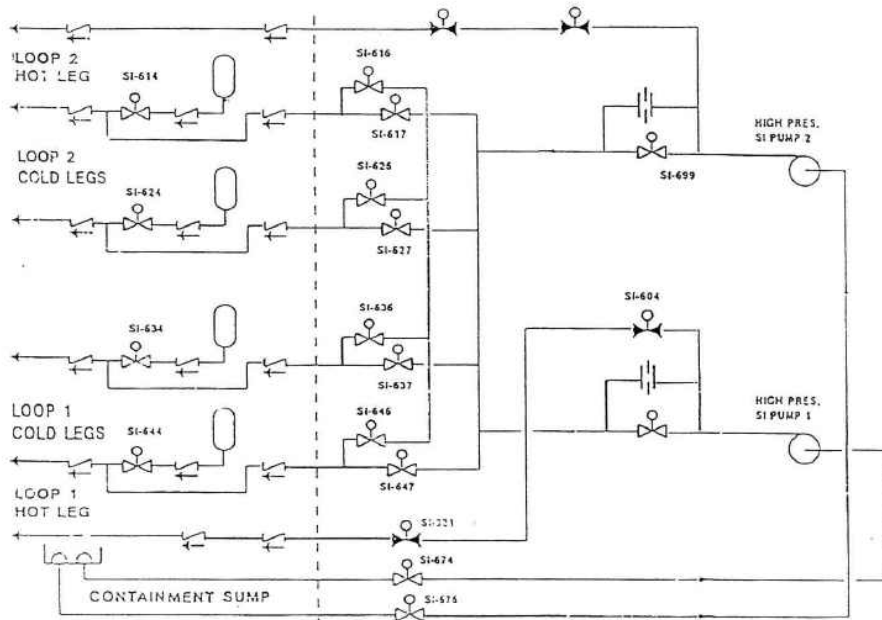


Figure 4.2 Alignment of ESF components of HPSIS in a recirculation mode

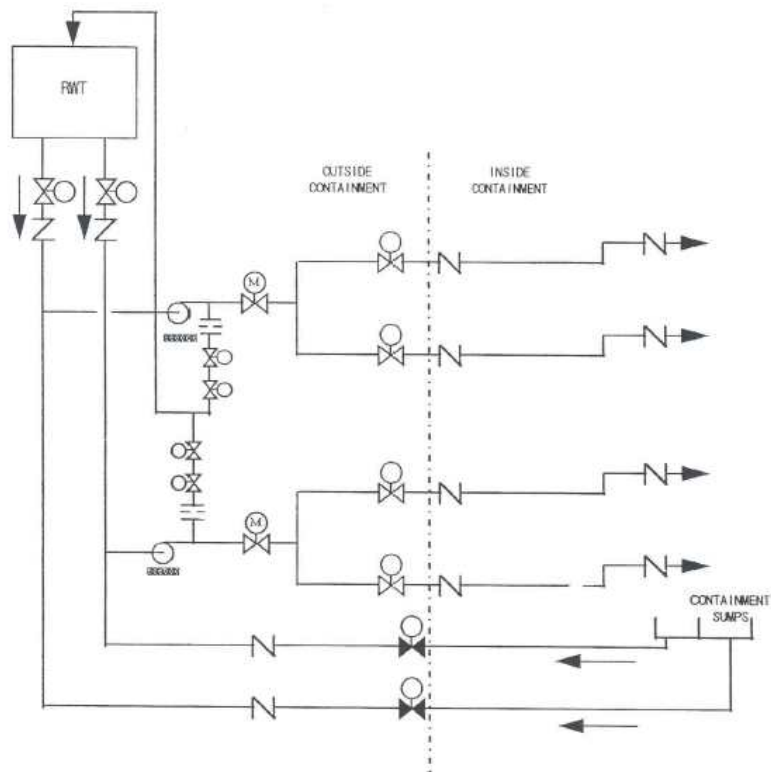


Figure 4.3 Alignment of ESF components of LPSIS in an injection mode

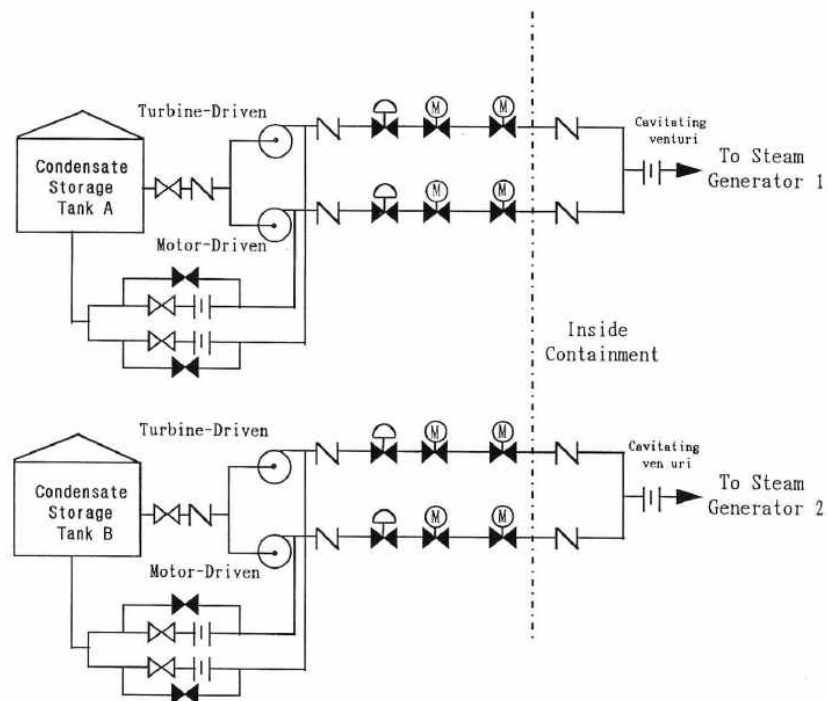


Figure 4.4 Alignment of ESF components of AFW system in an operational mode

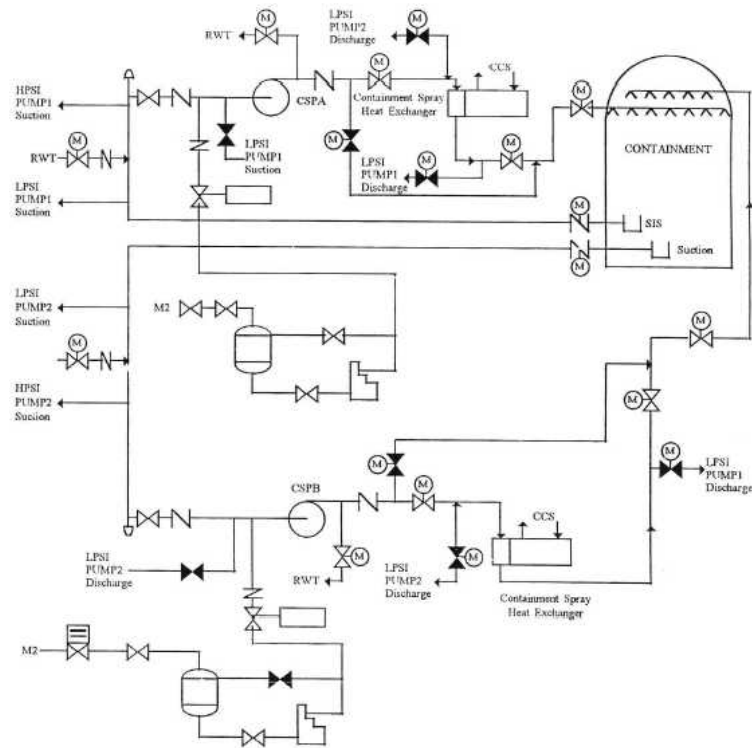


Figure 4.5 Alignment of ESF components of CS system in an injection mode

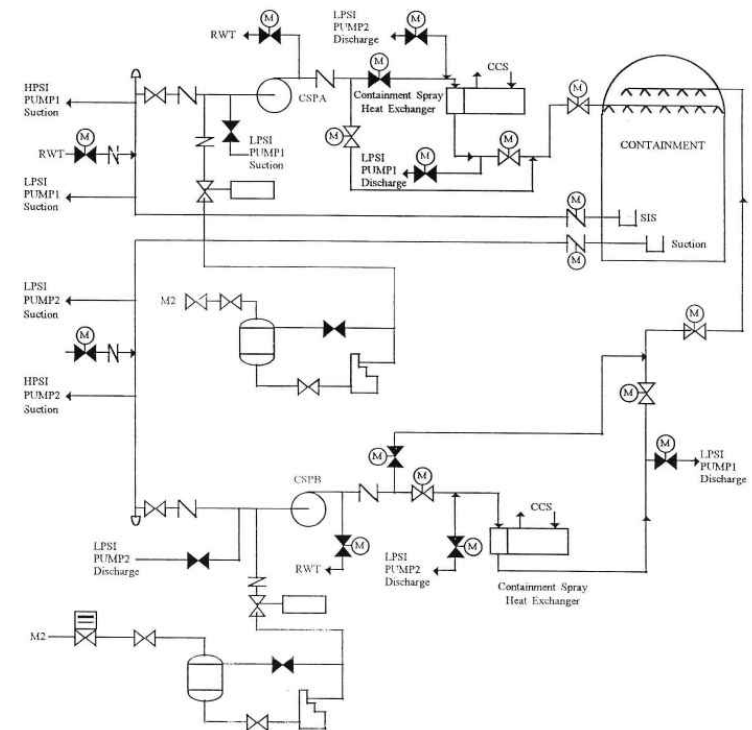


Figure 4.6 Alignment of ESF components of CS system in a recirculation mode

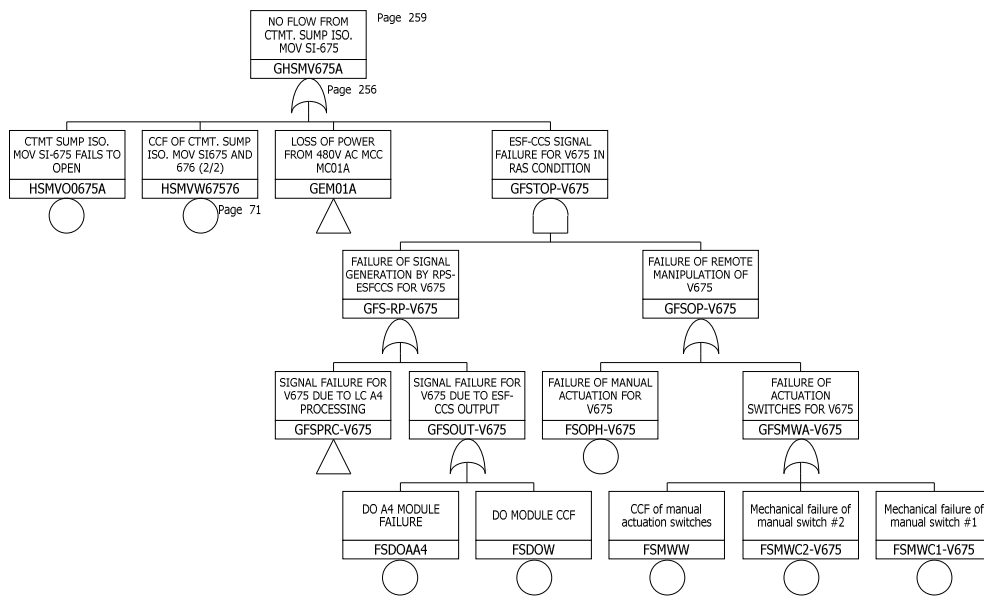


Figure 4.7 Logic of ESF-CCS signal failure for V675 in RAS condition

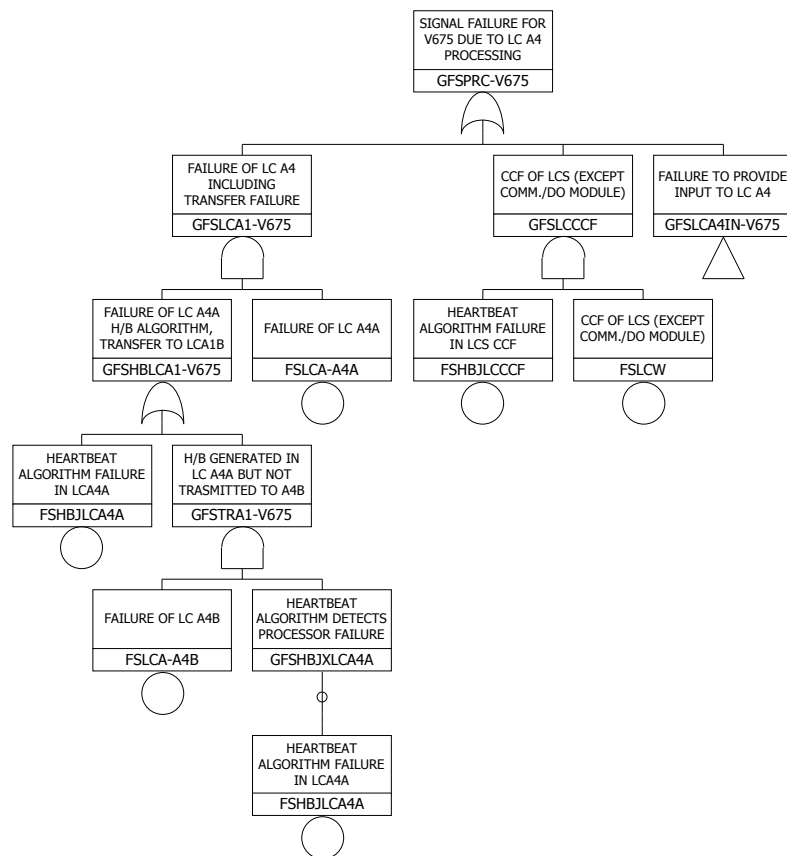


Figure 4.8 Logic of ESF actuation signal failure for V675 in RAS condition

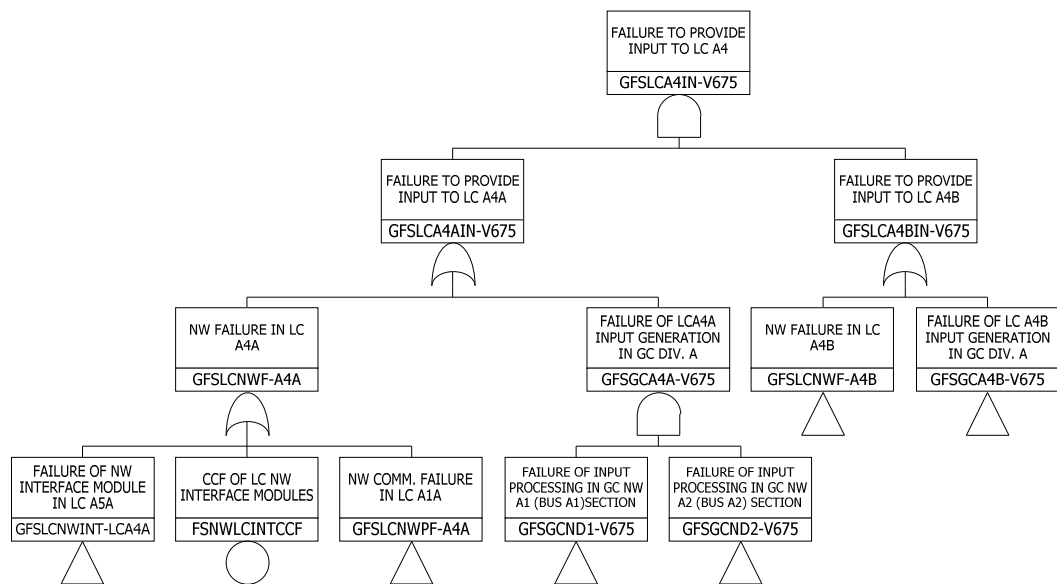


Figure 4.9 Logic of failure to provide input to LC A4A for V675 actuation

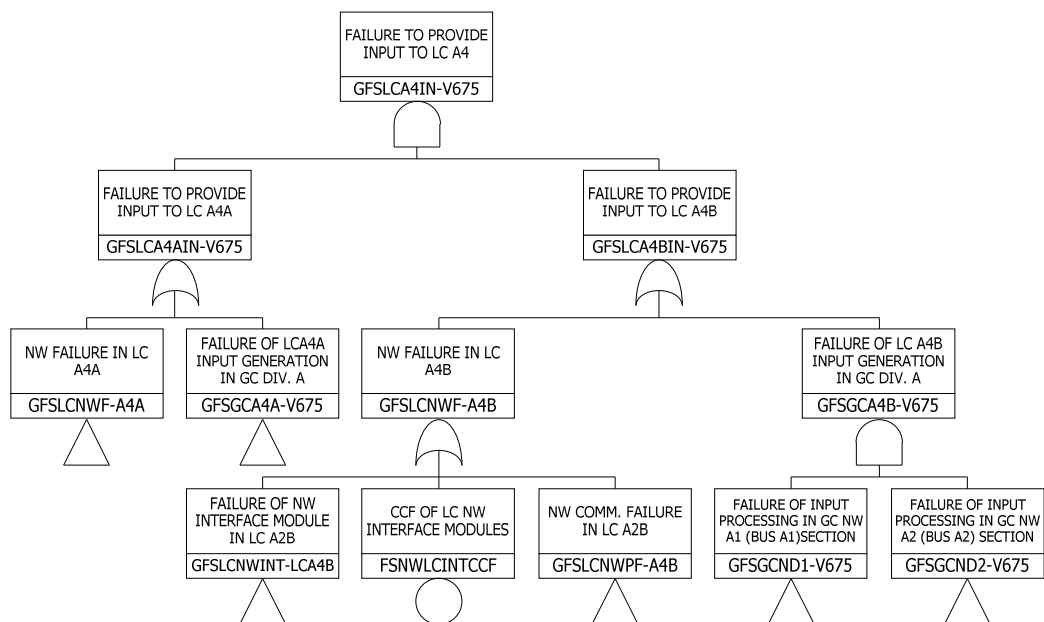


Figure 4.10 Logic of failure to provide input to LC A4B for V675 actuation

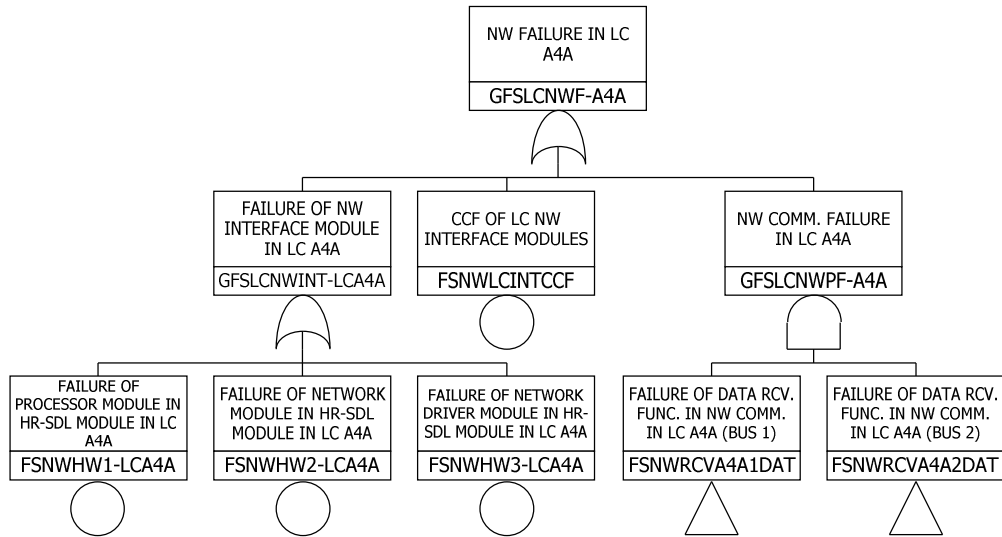


Figure 4.11 Logic of network failure in LC A4A
(including HR-SDL hardware component failure)

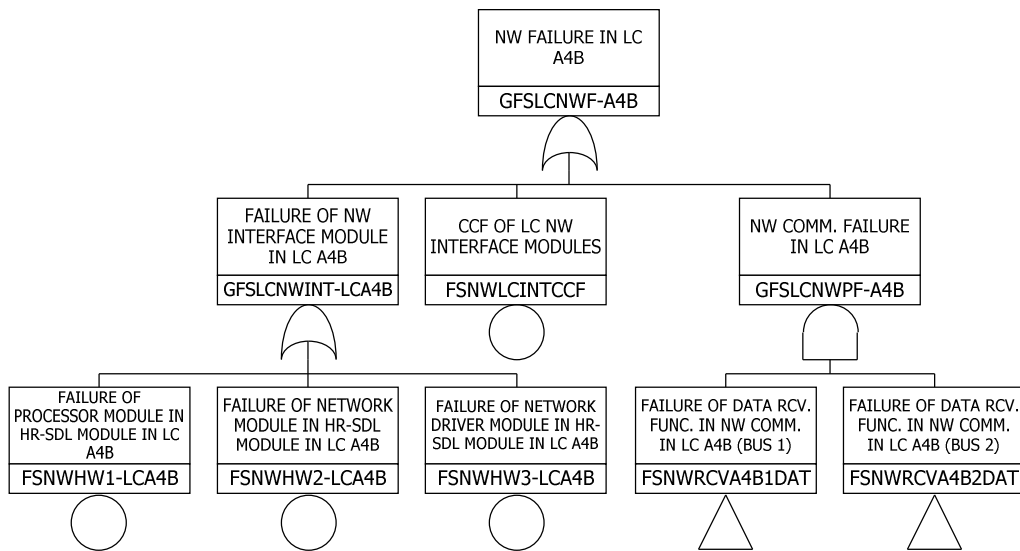


Figure 4.12 Logic of network failure in LC A4B
(including hardware component failure)

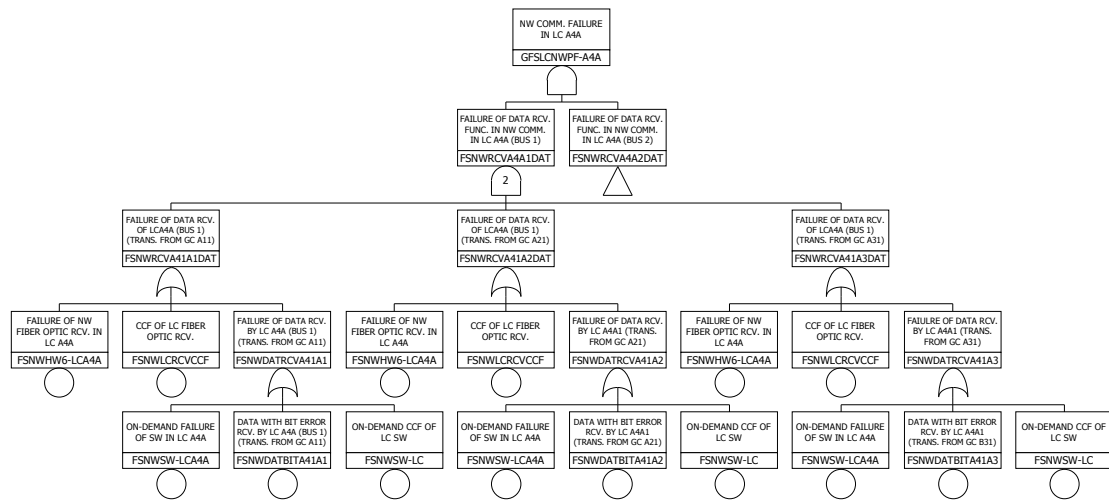


Figure 4.13 Logic of failure of network protocol (data reception failure) by LC A4A through network bus 1 transferred from GC

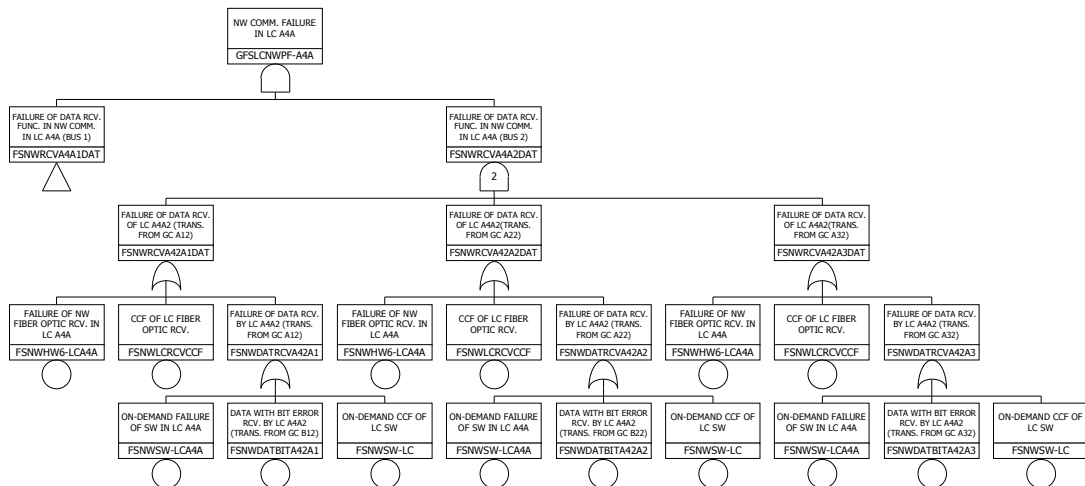


Figure 4.14 Logic of failure of network protocol (data reception failure) by LC A4A through network bus 2 transferred from GC

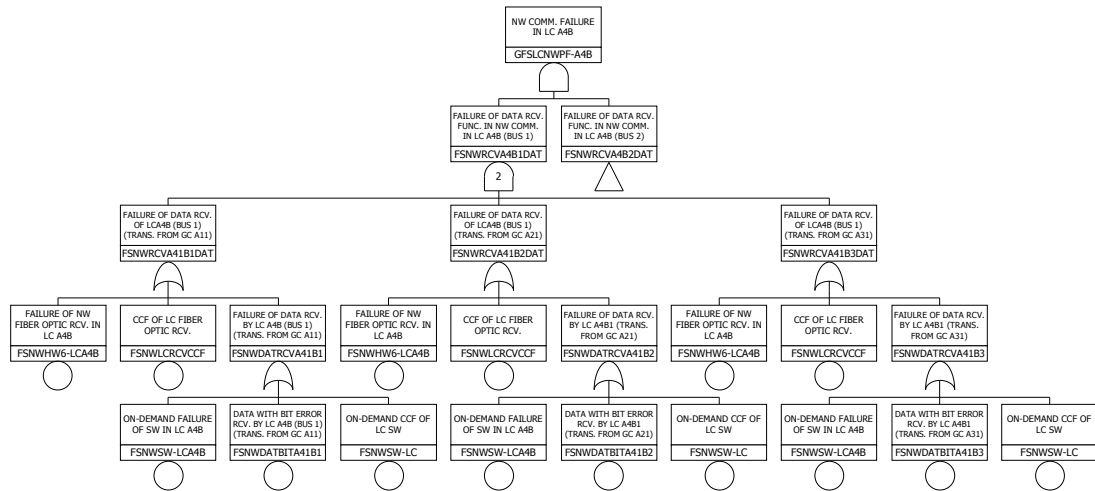


Figure 4.15 Logic of failure of network protocol (data reception failure) by LC A4B through network bus 1 transferred from GC

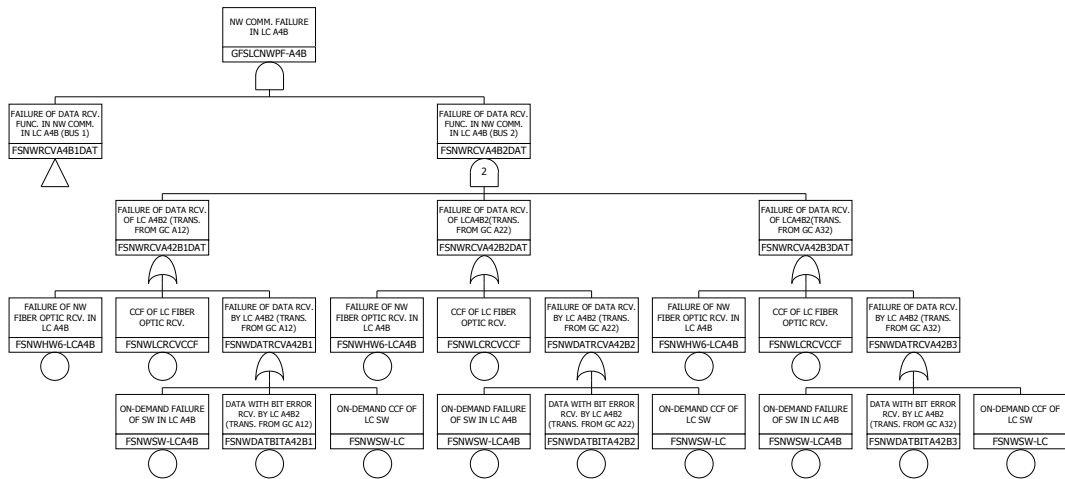


Figure 4.16 Logic of failure of network protocol (data reception failure) by LC A4B through network bus 2 transferred from GC

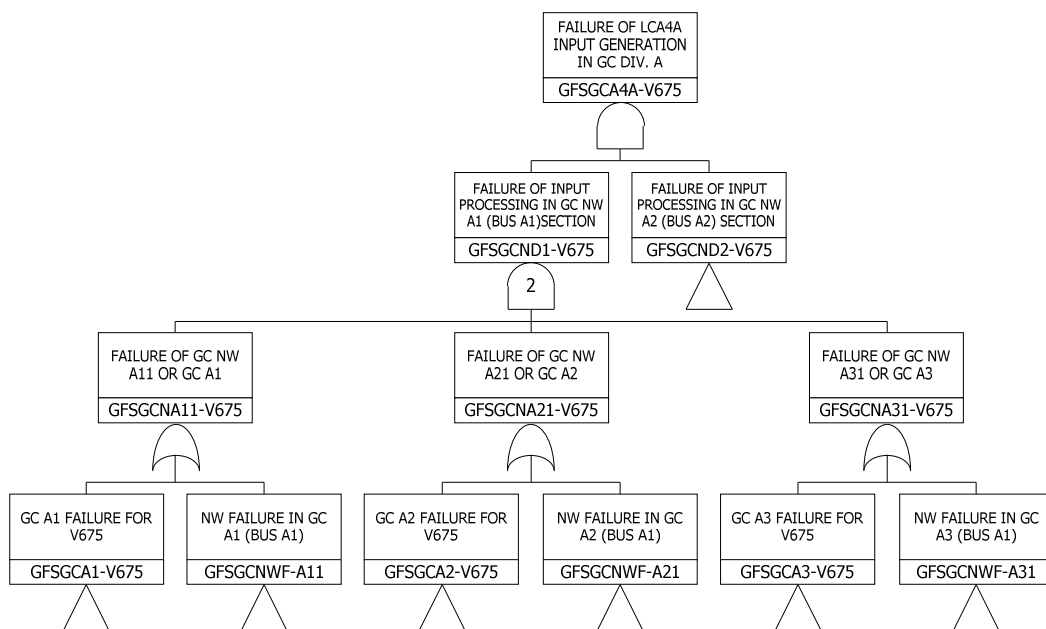


Figure 4.17 Logic of failure of LC A4A input generation by GCs (via network bus 1) in division A

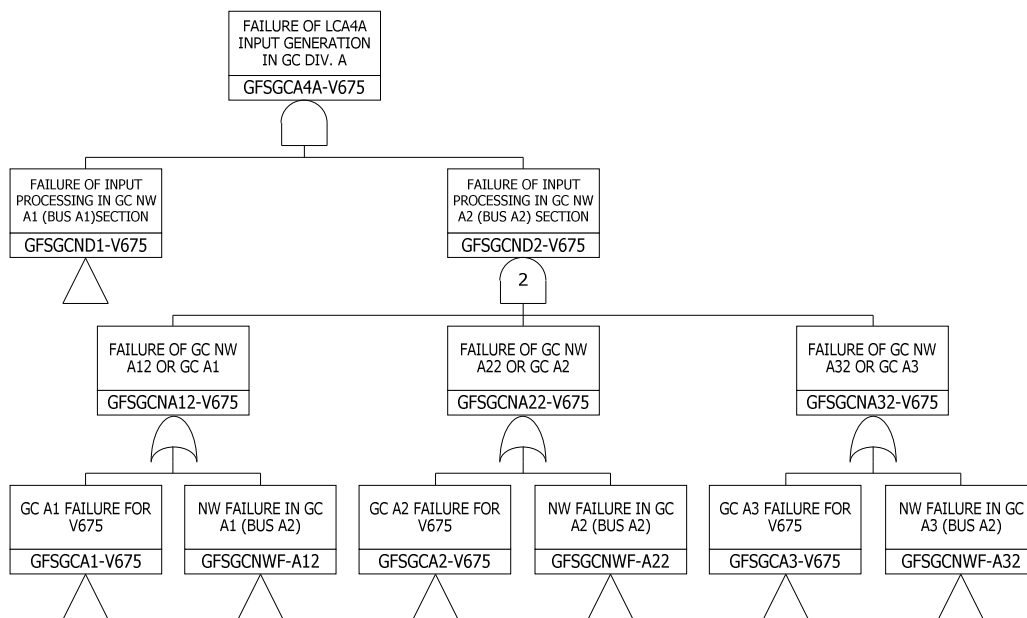


Figure 4.18 Logic of failure of LC A4A input generation by GCs (via network bus 2) in division A

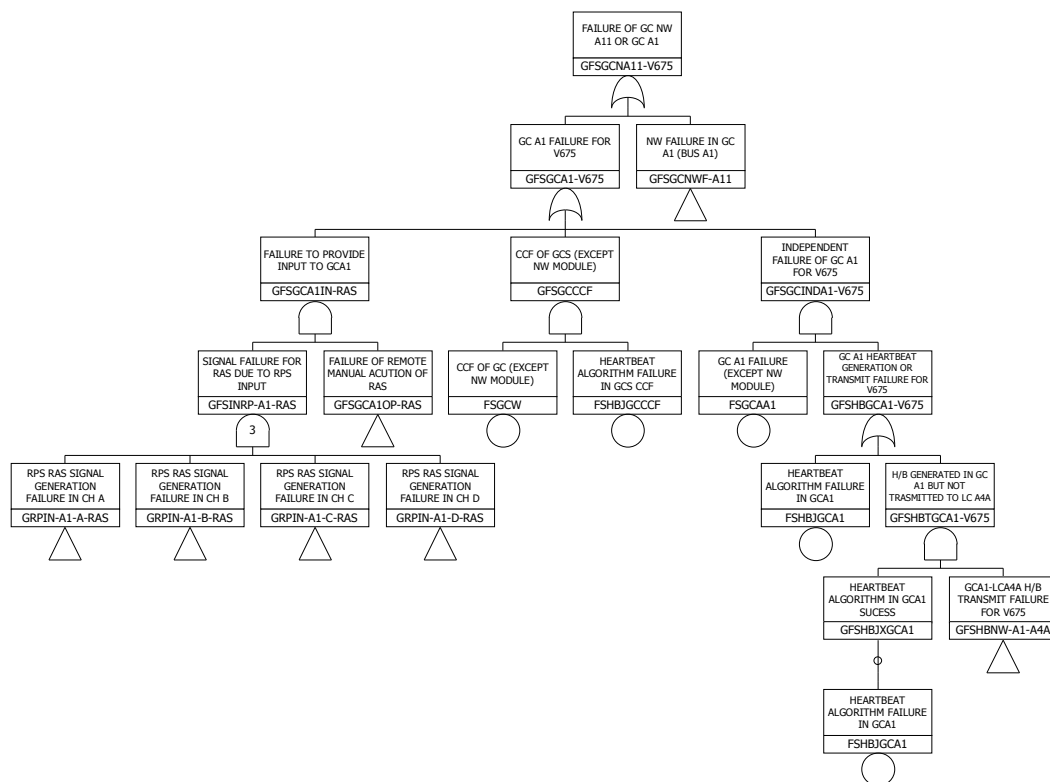


Figure 4.19 Logic of independent GC failure for V675 actuation (in the case of GC A1)

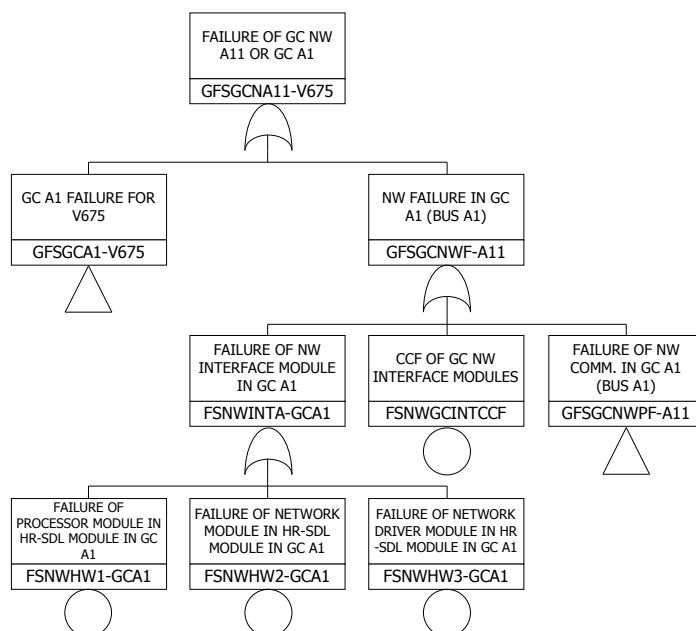


Figure 4.20 Logic of sub-level hardware component failure in network module of GC A1

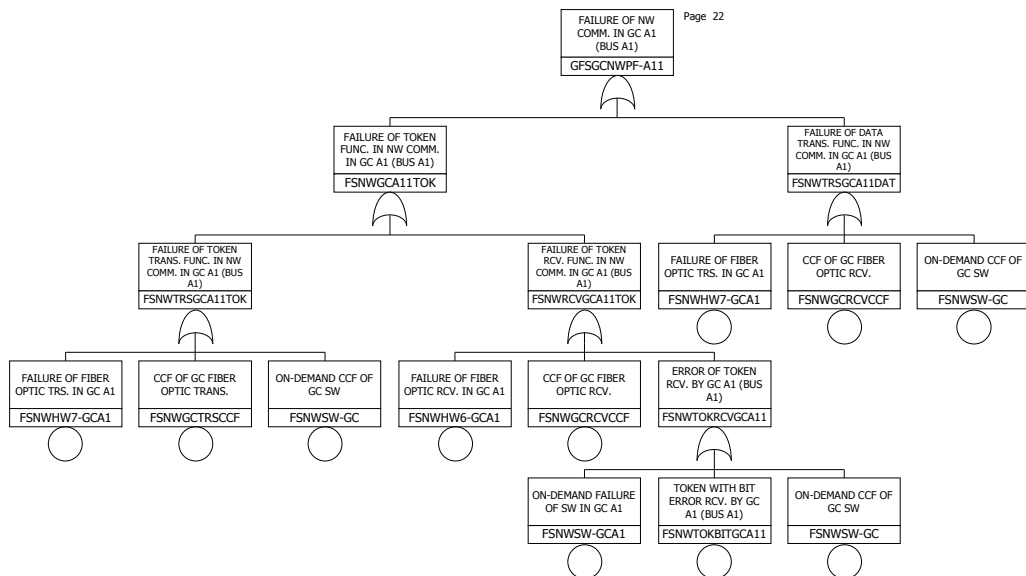


Figure 4.21 Logic of network failure in GC A1 through network bus A1

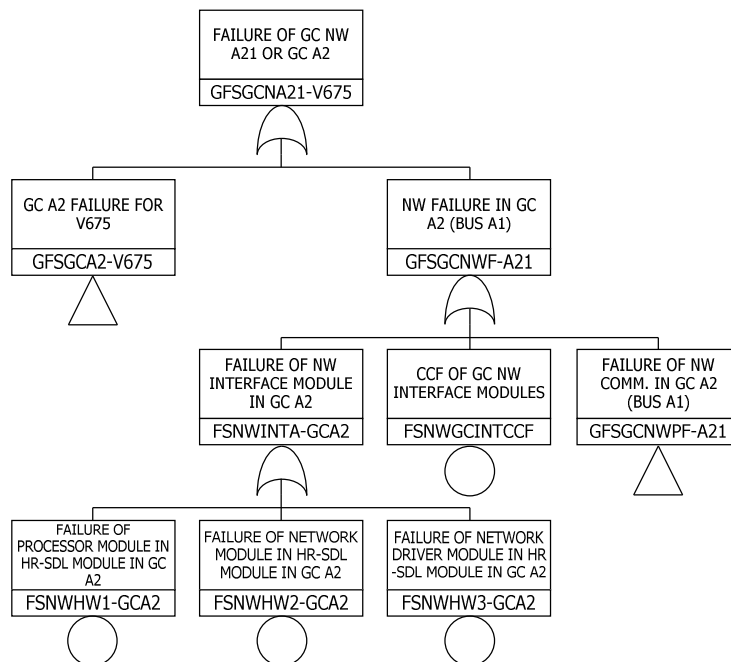


Figure 4.22 Logic of sub-level hardware component failure in network module of GC A2

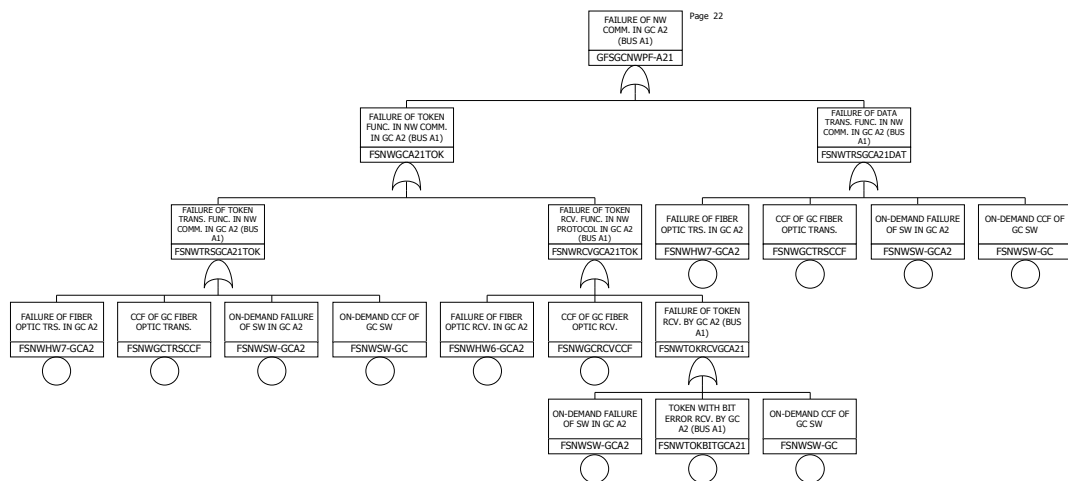


Figure 4.23 Logic of network failure in GC A2 through network bus A1

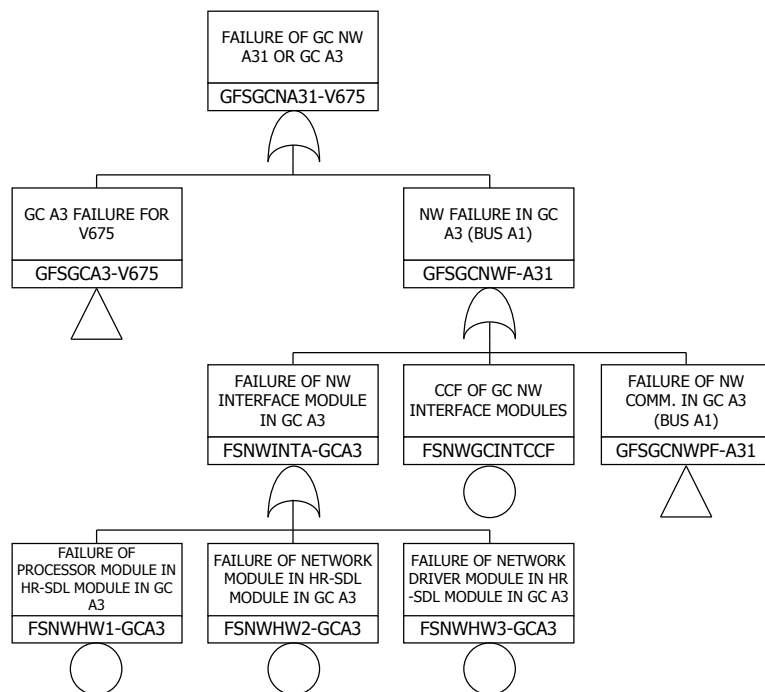


Figure 4.24 Logic of sub-level hardware component failure in network module of GC A3

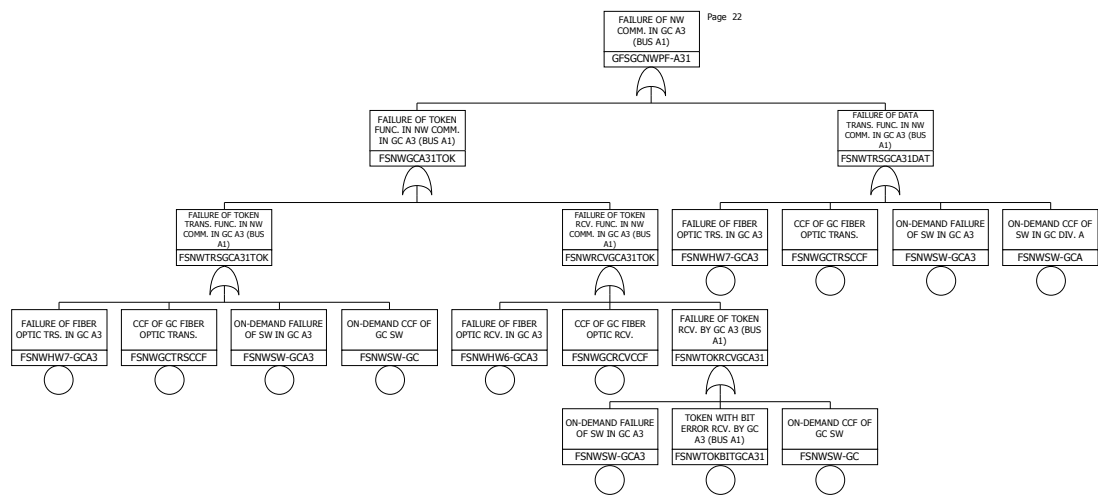


Figure 4.25 Logic of network failure in GC A3 through network bus A1

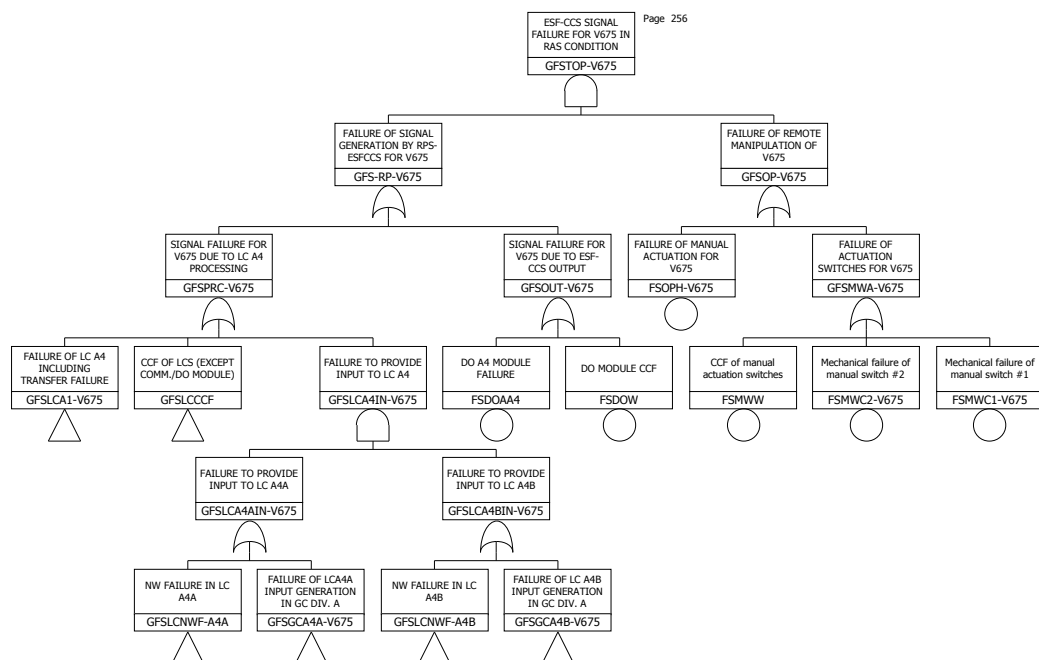


Figure 4.26 Logic of ESF-CCS signal failure for V675 in RAS condition

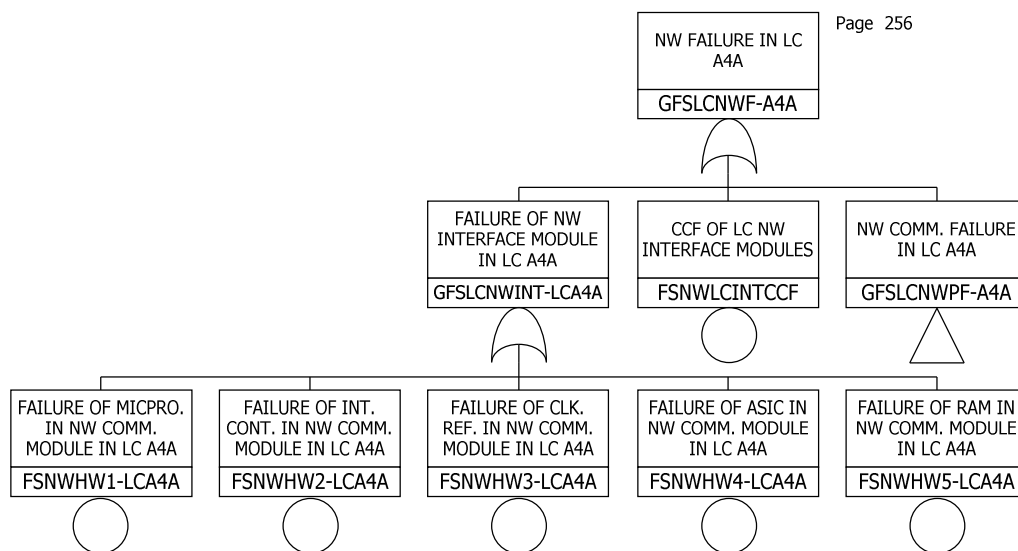


Figure 4.27 Logic of network failure in LC A4A
(including HR-SDN hardware component failure)

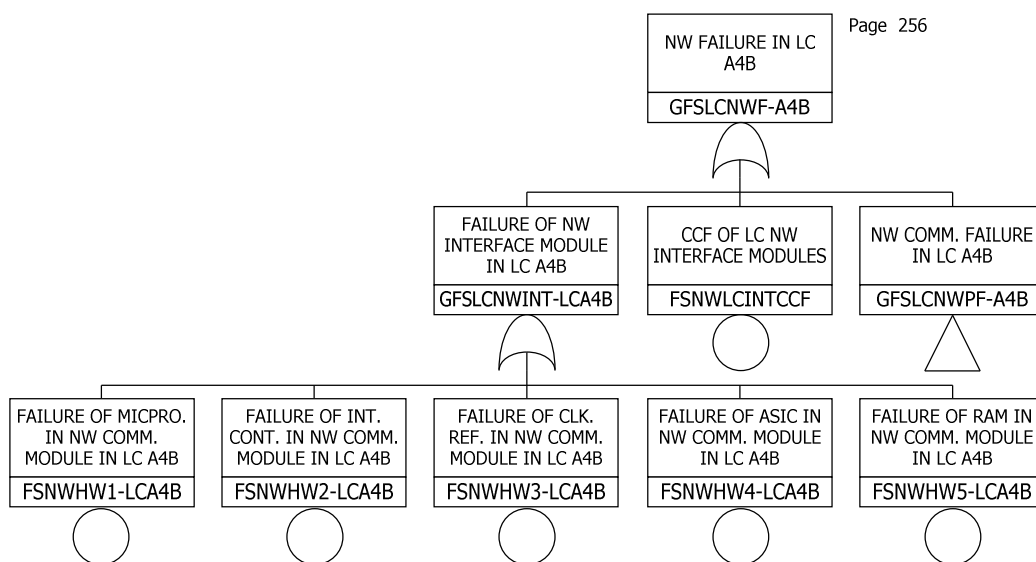


Figure 4.28 Logic of network failure in LC A4B
(including hardware component failure)

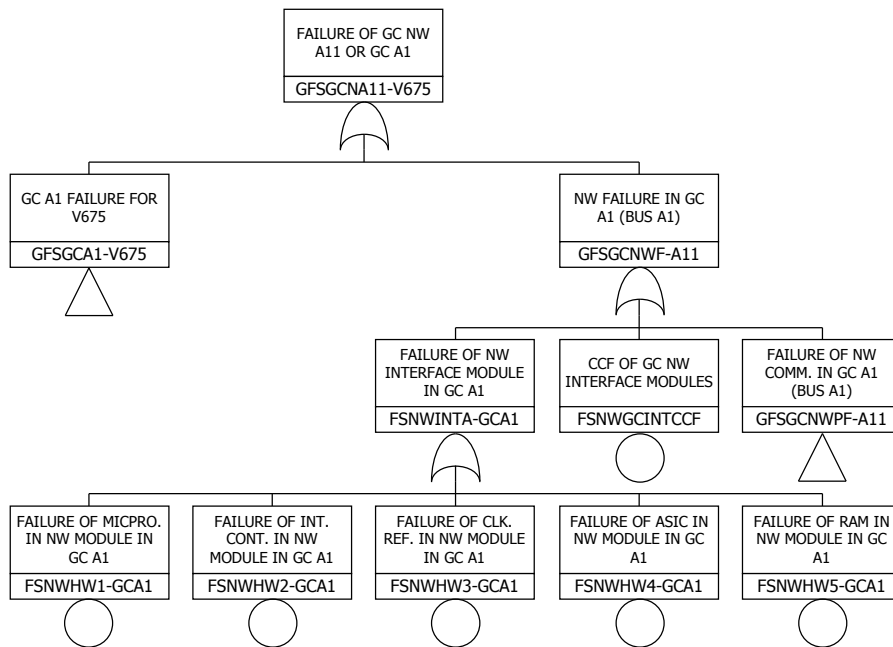


Figure 4.29 Logic of HR-SDN sub-level hardware component failure in network module of GC A1

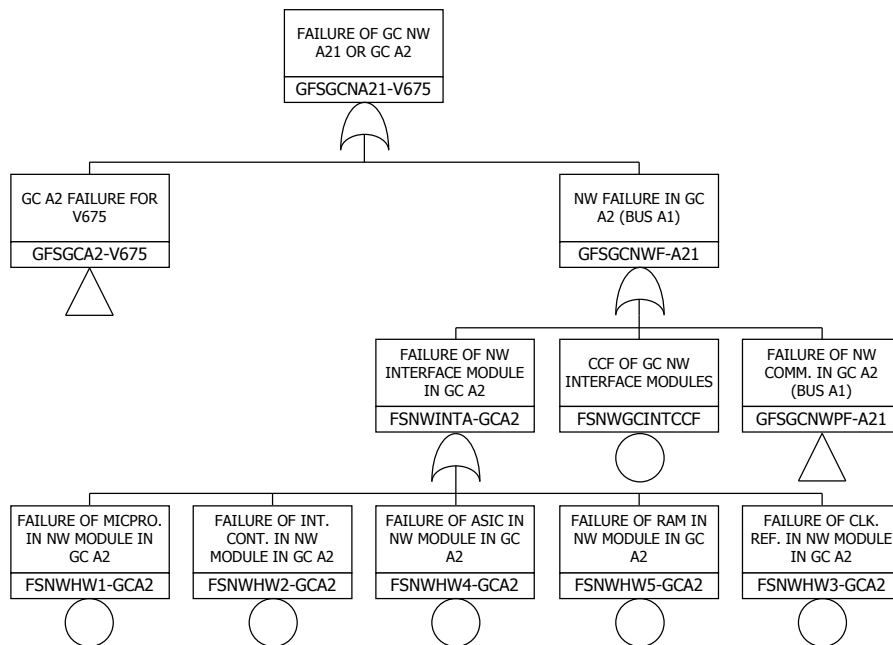


Figure 4.30 Logic of sub-level hardware component failure in network module of GC A2

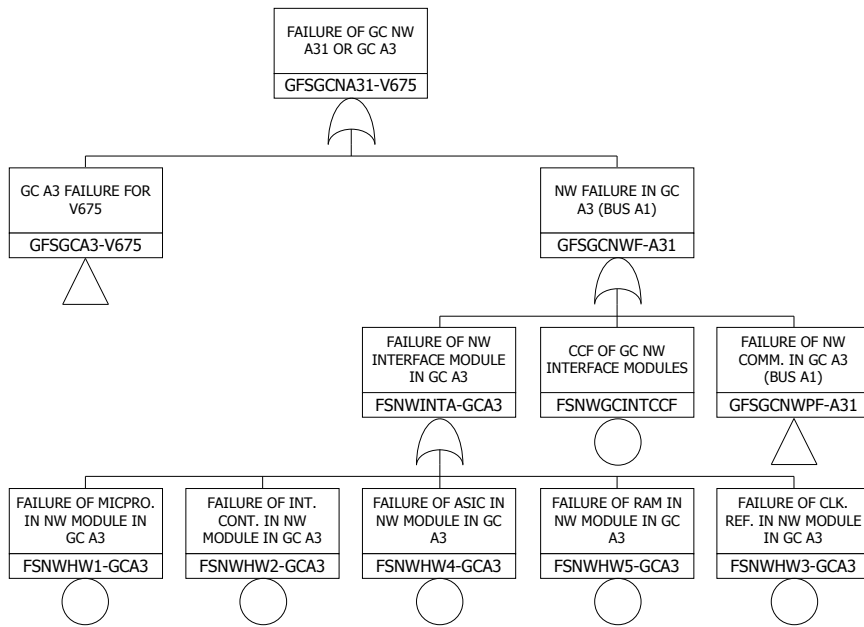


Figure 4.31 Logic of sub-level hardware component failure in network module of GC A3

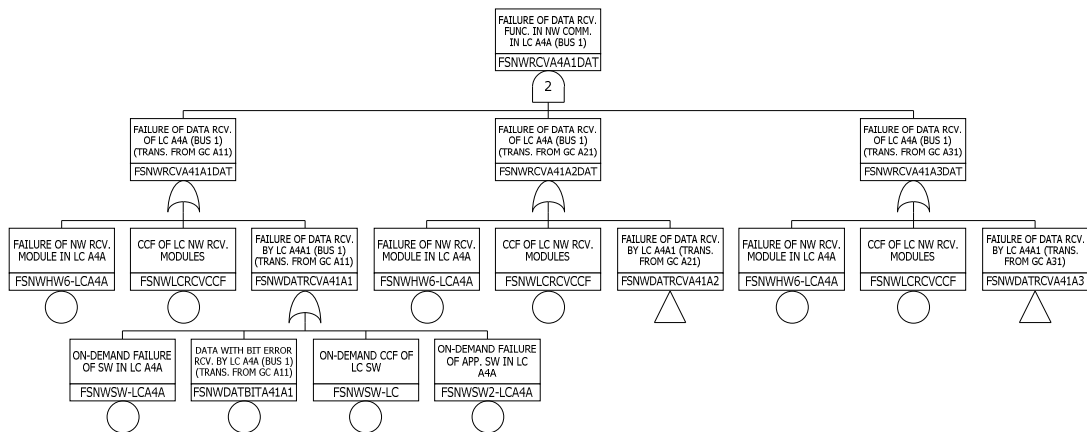


Figure 4.32 Logic of failure of network protocol (data reception failure) by LC A4A through network bus 1 transferred from GC

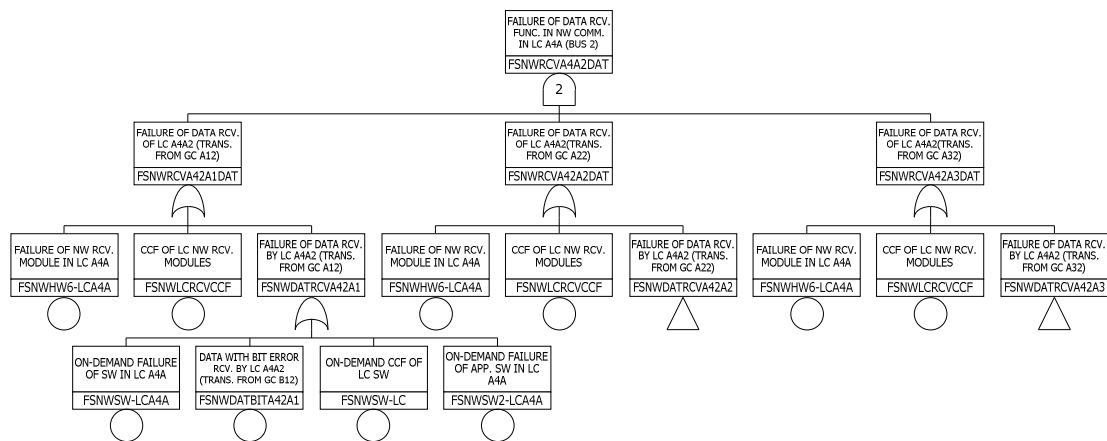


Figure 4.33 Logic of failure of network protocol (data reception failure) by LC A4A through network bus 2 transferred from GC

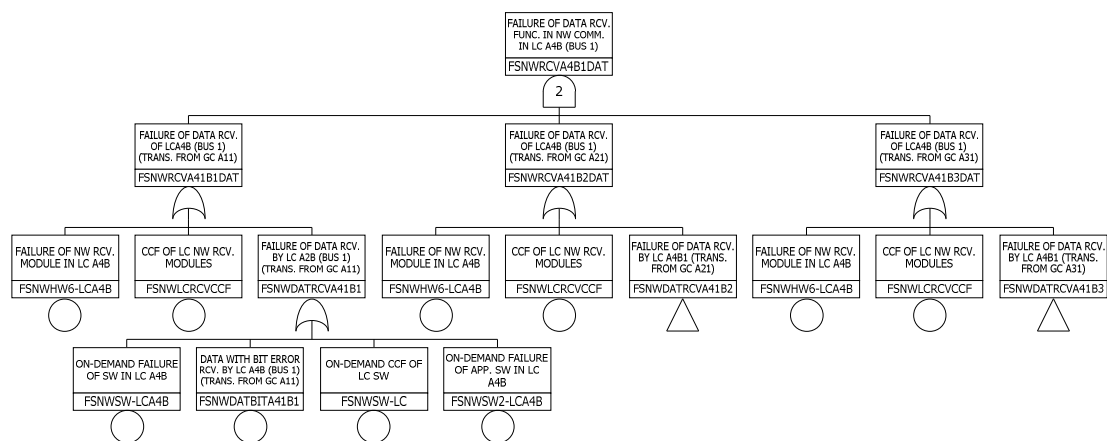


Figure 4.34 Logic of failure of network protocol (data reception failure) by LC A4B through network bus 1 transferred from GC

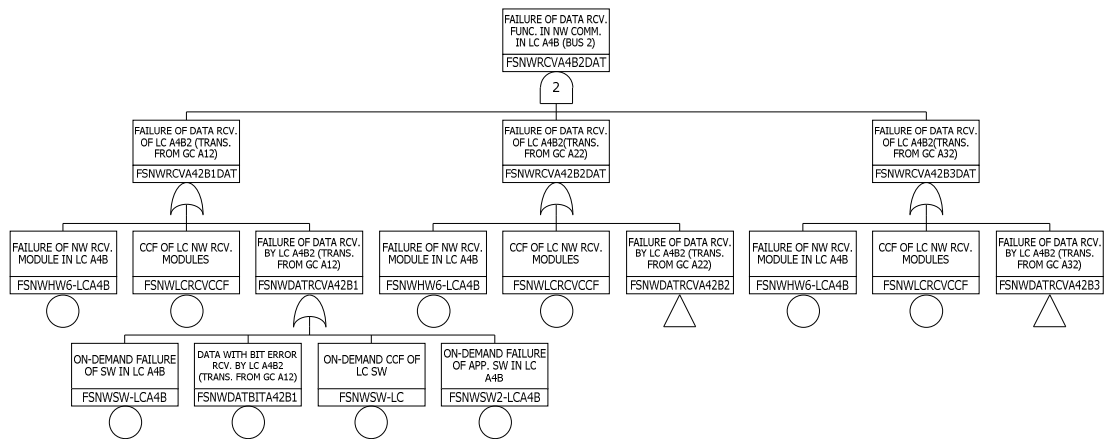


Figure 4.35 Logic of failure of network protocol (data reception failure) by LC A4B through network bus 2 transferred from GC

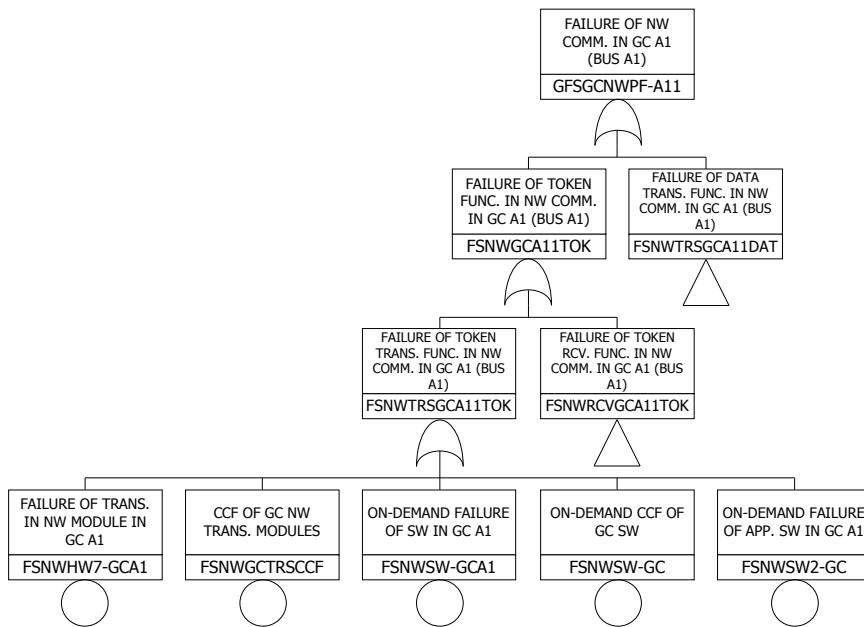


Figure 4.36 Logic of network failure (token transmission) in GC A1 through network bus A1

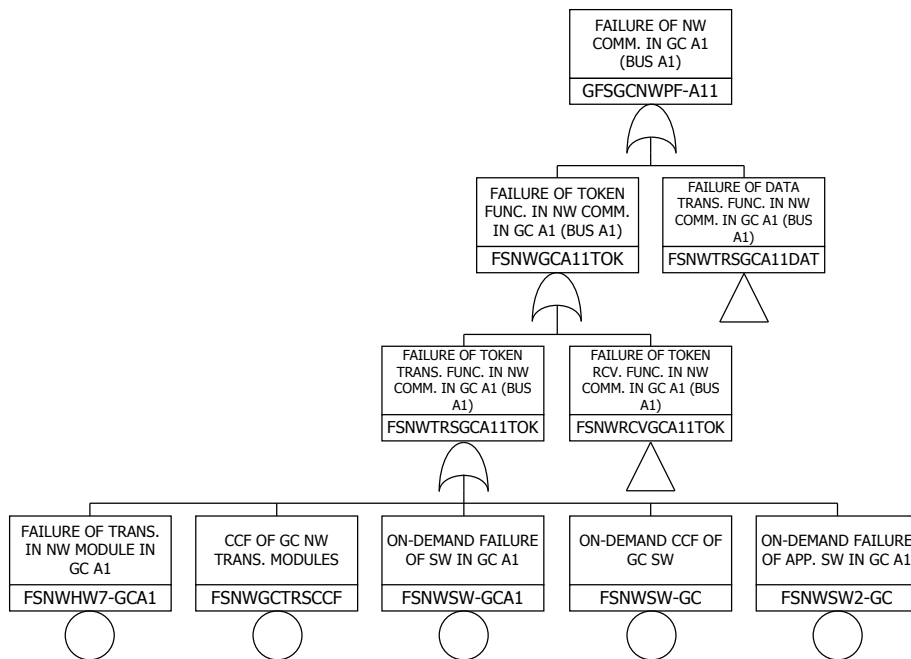


Figure 4.37 Logic of network failure (token reception) in GC A1 through network bus A1

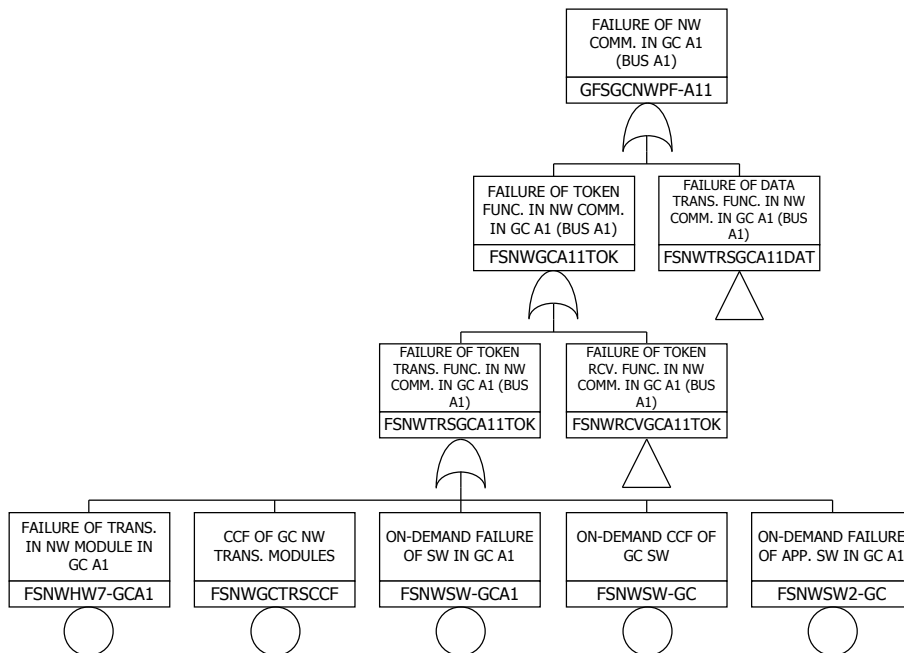


Figure 4.38 Logic of network failure (data transmission) in GC A1 through network bus A1

Chapter 5. Reliability Assessment of Network Communication

5.1 Sensitivity Study

To improve the reliability and availability of digital systems, testing strategies have been generally adopted in the digital systems. Especially, in the case of ESF-CCS, various tests for GCs and LCs are implemented through ETIP and COM [47]. ETIP takes charge of the passive and active test functions of the ESF-CCS and the interfaces of the ESF-CCS with other systems such as the reactor protection system and qualified indication and alarm system. The implemented tests can be classified into two categories, manual test and the automatic test. Active tests consist of automatic periodic tests, manual initiated automatic tests, and manual tests [89]. An automatic periodic test is periodically initiated by the ETIP without any human intervention. A manually initiated automatic test is almost the same as an automatic periodic test except for the operator initiation and tested parameter selection. This test is performed by a human decision, if necessary. A manual test is generally performed once per month. These tests, which can be complementary and overlapped to each other, cover the whole systems' function. Table 5.1 shows the test functions of ESF-CCS.

Based on the test functions implemented in ESF-CCS, three case studies were performed as a sensitivity study based on the periodic test methods for hardware components in GC and LC network module and their test intervals in this study. Three case studies include the manual testing, automatic testing by ETIP, and automatic testing by PLC scan of GC and LC network modules.

For manual testing, operators initiate the test for both local ESF manual actuation and individual component testing, including testing of the integrity of

network modules. The test interval for manual testing is assumed to be once per month (730 hours). In case of automatic periodic testing by ETIP, the test logic is performed using test signals for all functions of GC and LC; thus, testing the correct output or input to the GC and LC network modules. In this study, the test interval for automatic periodic testing by ETIP was assumed to be 8 hours based on the periodic test interval for digital reactor protection system [70]. In addition to the automatic testing by ETIP, the automatic testing by self-diagnostics function of PLC processor is considered in this study. Generally, a PLC program is executed repeatedly as part of a repetitive process referred to as a scan [74]. The general cycle of PLC self diagnostics are shown in Figure 5.1. As a PLC scan process, the status of physical input points is copied to an area of memory accessible to the processor. Once the PLC scan has been completed, the processor performs internal diagnostics and communication tasks at each PLC scan cycle. For example, data link error, or intra-channel network error, and faults such as a watchdog timer error can be detected by self-diagnostics. The overall PLC scan time is in the order of milliseconds, up to 100 milliseconds. Therefore, the periodic test interval of 50 milliseconds for automatic testing by PLC processor, or self-diagnostics function, is assumed. The detailed description of assumed test methods and their test interval is shown in Table 5.2.

Based on the quantification scheme for hardware failure mechanism, as shown in Equation (1), the unavailability of the hardware components were estimated and applied to the developed fault-tree model to quantify the risk effect of network failure on the plant risk.

5.2 Analysis of Minimal Cutsets related to Network Failure

In each case study, the dominant minimal cutsets (MCSs) related to network failure were analyzed to identify the plant hazard condition in case of network failure. Based on the one-top fault-tree model for OPR-1000 NPP, as shown in

Figure 5.2, the cutsets for plant CDF was generated using 'Kcut' cutset generator with the cutoff value of 1.00E-11. Based on the generated MCSs, the MCSs which contain nonsense cutsets, such as multiple channel failure due to maintenance, and double initiators were removed by post-processing.

5.2.1 Minimal Cutset Analysis for HR-SDL Network Communication

Based on the developed fault-tree model for HR-SDL network communication, the MCSs related to network failure were identified. Table 5.3 presents the dominant MCSs for the initiating event, small loss-of-coolant accident (SLOCA) where six different mitigation actions (i.e. HPSIS injection, Auxiliary feedwater deliver, LPSIS injection, HPSIS recirculation, LPSIS recirculation, Recirculation cooling by CS) requiring four different safety component actuation signal (i.e. SIAS, AFWS, RAS, CSAS), for case 1, where the manual testing with periodic test interval of 730 hours is assumed. Note that initiating event SLOCA requires largest number of mitigation actions which require safety component actuation signals compared to other initiating events.

As shown in Table 5.3, the important basic events in the dominant cut sets for ESF-CCS signal failure in case 1 relate to the digital component unavailability including the CCF of the hardware components in network modules, among others. Note that dominant MCSs related to network failure include failure of recirculation through two redundant train due to containment isolation MOVs (V675 and V676) fail to open in both channels. In addition, they include failure of HPSIS injection through two redundant trains due to the failure of HPSI pumps (HP02A, HP02B) to be operated in both channels. These MCSs related to network failure affect the unavailability of the ESF-CCS signal generation in combination with the manual actuation failure by human operator. The summary of the dominant MCSs related to network failure for case 1 is shown in Table 5.4.

In terms of case 2 and 3, where automatic periodic testing of the hardware

components in network module was assumed, low periodic test interval due to automatic periodic testing; thus, the software failure of GC and LC network modules is expected to have dominant effect on the CDF of the initiating event. Based on the cutset analysis result, as shown in Table 5.5 and 5.6, the dominant cut sets for ESF-CCS signal failure include the CCF of the software implemented in the network module in GC and LC for HR-SDL network communication.

5.2.2 Minimal Cutset Analysis for HR-SDN Network Communication

Based on the developed fault-tree model for HR-SDN network communication, the MCSs for initiating event SLOCA which include basic events related to network failure were identified. Table 5.7 presents the dominant MCSs for the initiating event SLOCA for case 1 where the manual testing with periodic test interval of 730 hours is assumed.

As shown in Table 5.7, the important basic events in the dominant cut sets for ESF-CCS signal failure in case 1 relate to the digital component unavailability including the CCF of the hardware components in network modules, among others. Note that the failure of application software in GC and LC network modules is considered in case of HR-SDN network communication. Therefore, in terms of software failure, the dominant MCSs related to network failure include the basic event regarding the failure of network module software and the failure of Application layer software. The summary of the dominant MCSs related to network failure for case 1 is shown in Table 5.8. In terms of case 2 and 3, where automatic periodic testing of the hardware components in network module was assumed, low periodic test interval due to automatic periodic testing; thus, the software failure of GC and LC network modules is expected to have dominant effect on the CDF of the initiating event. Based on the cutset analysis result, as shown in Table 5.9 and 5.10, the dominant cut sets for ESF-CCS signal failure include the CCF of both software implemented in the network module and the Application layer software in

GC and LC for HR-SDN network communication.

5.3 Analysis on the Risk Effect of Network Communication Failure

Based on the quantification results for each failure cause and identified MCSs based on fault-tree analysis in the three case studies, the risk effects of network failure on the initiating event SLOCA CD sequences were estimated. In this study, overall network failure risk was calculated as the sum of the failure probabilities of the hardware components, including the interface, receiver and transmitter modules; the probability of failure of software operation in the network module or Application layer software; and the probability of frame corruption caused by noise in the network medium. As shown in Table 5.3 ~ 5.10, which shows the dominant MCSs related to network failure, the probability value of MCSs related to the failure due to medium-related bit errors was negligible because of redundant GC and LC network modules along with the redundant network bus structure.

Based on the cutset analysis results for HR-SDL network communication, the CDF caused by the failure of network hardware components and the failure of software implemented in the network modules with the combination of operator's manual ESF actuation signal and the initiating event SLOCA frequency were $1.01\text{E-}07$ and $8.03\text{E-}10$, respectively in case 1. When assuming automatic periodic testing, where test interval is low compared to manual testing, the CDF caused by the failure of network hardware components and the failure of software implemented in the network modules with the combination of operator's manual ESF actuation signal and the initiating event SLOCA frequency were $1.10\text{E-}09$ and $8.03\text{E-}10$, respectively in case 2; and $2.01\text{E-}15$ and $8.03\text{E-}10$, respectively in case 3. The summary of sensitivity study results for the failure probability related to network modules in GC and LC are shown in Figure 5.3. In terms of risk effect of network failure on the SLOCA CD sequences, overall risk of network communication failure between GC and LC in ESF-CCS contributes up to 8.28% to the ESF component

actuation signal failure when manual testing for network hardware components are assumed. The detailed risk quantification results and the risk effect analysis for HR-SDL network communication is shown in Table 5.11.

In case of HR-SDN network communication, the software failure of Application layer is also considered in the fault-tree modeling for HR-SDN network module, while SW failure of CPB in FDL for HR-SDL network module is considered because HR-SDN is based on Profibus-DP protocol which utilizes both Data Link layer and Application layer with unconfigured connections and formatted data. In case 1, where the manual testing of network hardware components is assumed, the CDF caused by the failure of network hardware components and the failure of software implemented in the network modules with the combination of operator's manual ESF actuation signal and the initiating event SLOCA frequency were $1.78\text{E-}08$ and $1.03\text{E-}08$, respectively. When assuming automatic periodic testing, the CDF caused by the failure of network hardware components and the failure of software implemented in the network modules with the combination of operator's manual ESF actuation signal and the initiating event SLOCA frequency were $1.88\text{E-}10$ and $1.03\text{E-}08$, respectively in case 2; and $2.60\text{E-}16$ and $1.03\text{E-}8$, respectively in case 3. The summary of sensitivity study results for the failure probability related to network modules in GC and LC are shown in Figure 5.4. In terms of risk effect of network failure on the SLOCA CD sequences, overall risk of network communication failure between GC and LC in ESF-CCS contributes up to 2.41% to the ESF component actuation signal failure when manual testing for network hardware components are assumed. The detailed risk quantification results and the risk effect analysis for HR-SDN network communication is shown in Table 5.12.

In summary, Figure 5.5 shows the overview of the risk quantification results on various periodic test interval for both HR-SDL and HR-SDN system. The quantification results for both network protocol applied in network communication

between GC and LC in ESF-CCS revealed the potential application of HR-SDN network communication in NPP protection system compared to the conventional point-to-point data exchanging method such as HR-SDL network communication in terms of reliability. Considering the conventional testing of the modules in NPP protection systems, such as RPS and ESF-CCS; that is, manual periodic testing with the interval of 730 hours, application of HR-SDN for safety-critical signal exchange between GC and LC in ESF-CCS has the advantage in terms of reliability of the system, compared to the case of HR-SDL system, as shown in Table 5.11 and 5.12. The risk quantification results for both network communication system applied in ESF-CCS shows that the risk effect of network failure in case of HR-SDL system, which was estimated as 8.28%, is larger than that of HR-SDN system, which was estimated as 2.41%. This is because of high dependency of hardware component or module failure in Data Link layer for the case of HR-SDL network protocol, compared to the case of HR-SDN network protocol. Since HR-SDL is based on point-to-point data exchanging method, higher number of network and network driver modules along with the fiber optic transmitter and receiver are required while the network bus structure is implemented in HR-SDN network protocol; thus, reducing the number of required hardware components, such as transmitter and receiver.

In addition, the quantification results showed the advantage of implementing HR-SDL network protocol compared to HR-SDN network protocol when considering the automatic periodic testing of the network hardware components or modules. Although the coverage and capacity of automatic periodic testing of RPS and ESF-CCS module, where the hardware components are periodically tested in the interval of communication cycle of 50 ms, is not well investigated yet [20], when periodic testing of short test interval can be implemented in hardware components in HR-SDL and HR-SDN network modules, HR-SDL system has the advantage in terms of reliability because of relatively high reduction of unavailability due to hardware component failure compared to the case of HR-SDN system.

Table 5.1 Test functions of ESF-CCS

Test type		Test scope
Manual Test		Fan, door and temp. sensor test
		Manual actuation & reset test
		Individual component output test
Automatic Test	Passive Test	H/W self-diagnosis, Heartbeat error check
		GC ESF initiation signals comparison test
		LC ESF actuation signals comparison test
	Active Test	GC logic test
		LC actuation logic test
		LC component control logic test

Table 5.2 Description of sensitivity study cases for periodic test methods and their interval

Case	Test method	Description	Periodic test interval
1	Manual testing	Operator initiates the test for both local ESF manual actuation and individual component testing	T = 730 hours (once per a month)
2	Automatic periodic testing by ETIP	Using the test signals from ETIP, the test logic is performed using test signals for all functions of GC and LC.	T = 8 hours
3	Automatic periodic testing by self-diagnostics function of PLC processor	CPU performs internal diagnostics and communication tasks at each PLC scan cycle. Data link error/intra-channel network error can be detected by self-diagnostics.	T = 50 ms

Table 5.3 Dominant MCSs of IE SLOCA CD sequences
in case 1. for HR-SDL network communication

MCS #	Value	F-V	BE #1	BE #2	BE #3	BE #4	BE #5	BE #6
1	2.43E-07	1.98E-01	HSMVWGHDR	MXOPHDPLI	%U3-SL			
2	1.68E-07	1.37E-01	HSMVW67576	%U3-SL	NR-MV			
3	1.50E-07	1.22E-01	HSSPPSUMP	%U3-SL				
4	8.64E-08	7.03E-02	HSMPK00102	MXOPHDPLI	%U3-SL			
5	6.08E-08	4.95E-02	HCCQWHPP	MXOPHDPLI	%U3-SL			
6	6.01E-08	4.89E-02	HSMPW00102	MXOPHDPLI	%U3-SL			
7	5.65E-08	4.60E-02	HCCQKCCP	%U3-SL				
8	2.78E-08	2.26E-02	%U3-SL	FSNWLINTCCF	FSOPH-V675	FSOPH-V676		
9	2.78E-08	2.26E-02	%U3-SL	FSNWGCINTCCF	FSOPH-V675	FSOPH-V676		
10	1.91E-08	1.55E-02	HCCQKHPP	MXOPHDPLI	%U3-SL			
11	1.18E-08	9.60E-03	MXOPHDPLI	HCOPVCQHPPA	HCSKWHPP	%U3-SL	HCOPVCQHPPB-HD	
12	9.40E-09	7.60E-03	MXOPHDPLI	%U3-SL	FSNWLINTCCF	FSOPH-HP02A	FSOPH-HP02B	
13	9.40E-09	7.60E-03	MXOPHDPLI	%U3-SL	FSNWGCINTCCF	FSOPH-HP02A	FSOPH-HP02B	
14	9.39E-09	7.60E-03	EOSYFTRIP	EGDGR01A	EGDGR01E	EGDGR01B	%U3-SL	NR-AC2HR
15	9.12E-09	7.40E-03	HSMVO0675A	HSMVO0676B	%U3-SL	NR-MV		
16	8.83E-09	7.20E-03	EOSYFTRIP	EGDGK01ABET	%U3-SL	NR-AC2HR		
17	8.56E-09	7.00E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWGTRSCCF		
18	7.85E-09	6.40E-03	HSMPK00102	MXOPHDPLR	%U3-SL			
19	7.20E-09	5.90E-03	CVTKBRWT00	%U3-SL				
20	6.49E-09	5.30E-03	%U3-SL	FSDOW	FSOPH-V675	FSOPH-V676		
21	6.24E-09	5.10E-03	CVCVW30506	%U3-SL				
22	6.24E-09	5.10E-03	HSCVW20506	%U3-SL				
23	5.53E-09	4.50E-03	HCCQWHPP	MXOPHDPLR	%U3-SL			
24	5.46E-09	4.40E-03	HSMPW00102	MXOPHDPLR	%U3-SL			
25	5.31E-09	4.30E-03	%U3-SL	FSDIW	FSOPH-V675	FSOPH-V676		
26	5.26E-09	4.30E-03	%U3-SL	CWCUK1A1BD	CWCUK2A2BD			
27	5.05E-09	4.10E-03	HSCVWG540123	%U3-SL				
28	5.05E-09	4.10E-03	HSCVWG212347	%U3-SL				
29	4.53E-09	3.70E-03	HSMPM0002B	HCCQMHPA	MXOPHDPLI	%U3-SL		
30	4.53E-09	3.70E-03	HCCQMHPB	HSMPM0001A	MXOPHDPLI	%U3-SL		
31	3.84E-09	3.10E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWGCRCVCCF		
32	3.84E-09	3.10E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWLRCVCCF		
33	3.09E-09	2.50E-03	HSMPR0002B	HCCQMHPA	MXOPHDPLI	%U3-SL		
34	3.09E-09	2.50E-03	HCCQMHPB	HSMPR0001A	MXOPHDPLI	%U3-SL		
35	2.89E-09	2.40E-03	MXOPHDPLI	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWGTRSCCF	
36	2.64E-09	2.10E-03	%U3-SL	CWCUK1A1BD	CWCUK2A2BD			
37	2.20E-09	1.80E-03	MXOPHDPLI	%U3-SL	FSDOW	FSOPH-HP02A	FSOPH-HP02B	
38	2.14E-09	1.70E-03	HSMPR0002B	HSMPM0001A	MXOPHDPLI	%U3-SL		
39	2.14E-09	1.70E-03	HSMPM0002B	HSMPR0001A	MXOPHDPLI	%U3-SL		
40	2.11E-09	1.70E-03	HSCVW40405	MXOPHDPLI	%U3-SL			

Table 5.4 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 1. for HR-SDL network communication

Value	F-V	BE #1	BE #2	BE #3	BE #4	BE #5
2.78E-08	2.26E-02	%U3-SL	FSNWL CINTCC F	FSOPH-V675	FSOPH-V676	
2.78E-08	2.26E-02	%U3-SL	FSNWGCINTCC F	FSOPH-V675	FSOPH-V676	
9.40E-09	7.60E-03	MXOPHDPLI	%U3-SL	FSNWL CINTCC F	FSOPH-HP02A	FSOPH-HP02B
9.40E-09	7.60E-03	MXOPHDPLI	%U3-SL	FSNWGCINTCC F	FSOPH-HP02A	FSOPH-HP02B
8.56E-09	7.00E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWGCTRSCCF	
3.84E-09	3.10E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWGCRCVCCF	
3.84E-09	3.10E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWL CRCVCCF	
2.89E-09	2.40E-03	MXOPHDPLI	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWGCTRSCCF
1.30E-09	1.10E-03	MXOPHDPLI	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWL CRCVCCF
1.30E-09	1.10E-03	MXOPHDPLI	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWGCRCVCCF
8.54E-10	7.00E-04	MXOPHDPL R	%U3-SL	FSNWL CINTCC F	FSOPH-V676	FSOPH-HP02A
8.54E-10	7.00E-04	MXOPHDPL R	%U3-SL	FSNWL CINTCC F	FSOPH-V675	FSOPH-HP02B
8.54E-10	7.00E-04	MXOPHDPL R	%U3-SL	FSNWGCINTCC F	FSOPH-HP02A	FSOPH-HP02B
8.54E-10	7.00E-04	MXOPHDPL R	%U3-SL	FSNWGCINTCC F	FSOPH-V676	FSOPH-HP02A
8.54E-10	7.00E-04	MXOPHDPL R	%U3-SL	FSNWL CINTCC F	FSOPH-HP02A	FSOPH-HP02B
8.54E-10	7.00E-04	MXOPHDPL R	%U3-SL	FSNWGCINTCC F	FSOPH-V675	FSOPH-HP02B
3.00E-10	2.00E-04	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWSW-GC	
3.00E-10	2.00E-04	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWSW-LC	
1.01E-10	6.67E-05	MXOPHDPLI	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWSW-GC
1.01E-10	6.67E-05	MXOPHDPLI	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWSW-LC

Table 5.5 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 2. for HR-SDL network communication

Value	F-V	BE #1	BE #2	BE #3	BE #4	BE #5
3.05E-10	2.73E-04	%U3-SL	FSNWGCINTCCF	FSOPH-V675	FSOPH-V676	
3.05E-10	2.73E-04	%U3-SL	FSNWLCINTCCF	FSOPH-V675	FSOPH-V676	
3.00E-10	2.69E-04	FSOPH-V675	FSOPH-V676	FSNWSW-LC		
3.00E-10	2.69E-04	FSOPH-V675	FSOPH-V676	FSNWSW-GC		
1.03E-10	9.22E-05	%U3-SL	FSNWGCINTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.03E-10	9.22E-05	%U3-SL	FSNWLCINTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.01E-10	9.08E-05	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWSW-GC	
1.01E-10	9.08E-05	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWSW-LC	
9.38E-11	8.40E-05	%U3-SL	FSNWGCTRSCCF	FSOPH-V675	FSOPH-V676	
4.21E-11	3.77E-05	%U3-SL	FSNWGCRCVCCF	FSOPH-V675	FSOPH-V676	
4.21E-11	3.77E-05	%U3-SL	FSNWLCRCVCCF	FSOPH-V675	FSOPH-V676	
3.17E-11	2.84E-05	%U3-SL	FSNWGCTRSCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.42E-11	1.27E-05	%U3-SL	FSNWGCRCVCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.42E-11	1.27E-05	%U3-SL	FSNWLCRCVCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.22E-11	1.09E-05	%U3-SL	FSNWGCINTCCF	FSOPH-V676	HSMVO0675A	
1.22E-11	1.09E-05	%U3-SL	FSNWGCINTCCF	FSOPH-V675	HSMVO0676B	
1.22E-11	1.09E-05	%U3-SL	FSNWLCINTCCF	FSOPH-V676	HSMVO0675A	
1.22E-11	1.09E-05	%U3-SL	FSNWLCINTCCF	FSOPH-V675	HSMVO0676B	

Table 5.6 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 3. for HR-SDL network communication

Value	F-V	BE #1	BE #2	BE #3	BE #4	BE #5
3.00E-10	2.69E-04	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWSW-LC	
3.00E-10	2.69E-04	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWSW-GC	
1.01E-10	9.09E-05	MXOPHDPLI	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWSW-GC
1.01E-10	9.09E-05	MXOPHDPLI	%U3-SL	FSOPH-HP02A	FSOPH-HP02B	FSNWSW-LC
5.29E-16	4.74E-10	%U3-SL	FSNWGCINTCCF	FSOPH-V675	FSOPH-V676	
5.29E-16	4.74E-10	%U3-SL	FSNWLCONTCCF	FSOPH-V675	FSOPH-V676	
1.79E-16	1.60E-10	%U3-SL	FSNWGCINTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.79E-16	1.60E-10	%U3-SL	FSNWLCONTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.63E-16	1.46E-10	%U3-SL	FSNWGCINTCCF	FSOPH-V675	FSOPH-V676	
7.31E-17	6.55E-11	%U3-SL	FSNWLRCVCCF	FSOPH-V675	FSOPH-V676	
7.31E-17	6.55E-11	%U3-SL	FSNWGCINTCCF	FSOPH-V675	FSOPH-V676	
5.51E-17	4.93E-11	%U3-SL	FSNWGCINTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
2.47E-17	2.22E-11	%U3-SL	FSNWLRCVCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
2.47E-17	2.22E-11	%U3-SL	FSNWGCINTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
2.12E-17	1.90E-11	%U3-SL	FSNWGCINTCCF	FSOPH-V676	HSMVO0675A	
2.12E-17	1.90E-11	%U3-SL	FSNWGCINTCCF	FSOPH-V675	HSMVO0676B	
2.12E-17	1.90E-11	%U3-SL	FSNWLCONTCCF	FSOPH-V676	HSMVO0675A	
2.12E-17	1.90E-11	%U3-SL	FSNWLCONTCCF	FSOPH-V675	HSMVO0676B	
1.63E-17	1.46E-11	%U3-SL	FSNWGCINTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLR
1.63E-17	1.46E-11	%U3-SL	FSNWGCINTCCF	FSOPH-HP02A	FSOPH-V676	MXOPHDPLR
1.63E-17	1.46E-11	%U3-SL	FSNWGCINTCCF	FSOPH-HP02B	FSOPH-V675	MXOPHDPLR
1.63E-17	1.46E-11	%U3-SL	FSNWLCONTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLR
1.63E-17	1.46E-11	%U3-SL	FSNWLCONTCCF	FSOPH-HP02A	FSOPH-V676	MXOPHDPLR
1.63E-17	1.46E-11	%U3-SL	FSNWLCONTCCF	FSOPH-HP02B	FSOPH-V675	MXOPHDPLR

Table 5.7 Dominant MCSs of IE SLOCA CD sequences
in case 1. for HR-SDN network communication

MCS #	Value	F-V	BE #1	BE #2	BE #3	BE #4	BE #5	BE #6
1	2.43E-07	2.13E-01	HSMVWGHDR	MXOPHDPLI	%U3-SL			
2	1.68E-07	1.47E-01	HSMVW67576	%U3-SL	NR-MV			
3	1.50E-07	1.31E-01	HSSPPSUMP	%U3-SL				
4	8.64E-08	7.57E-02	HSMPK00102	MXOPHDPLI	%U3-SL			
5	6.08E-08	5.33E-02	HCCQWHPP	MXOPHDPLI	%U3-SL			
6	6.01E-08	5.27E-02	HSMPW00102	MXOPHDPLI	%U3-SL			
7	5.65E-08	4.95E-02	HCCQKCCP	%U3-SL				
8	1.91E-08	1.67E-02	HCCQKHPP	MXOPHDPLI	%U3-SL			
9	1.18E-08	1.03E-02	MXOPHDPLI	HCOPVCQHPP A	HCSKWHPP	%U3-SL	HCOPVCQHPP B-HD	
10	9.39E-09	8.20E-03	EOSYFTRIP	EGDGR01A	EGDGR01E	EGDGR01B	%U3-SL	NR-AC2HR
11	9.12E-09	8.00E-03	HSMVO0675A	HSMVO0676B	%U3-SL	NR-MV		
12	8.83E-09	7.70E-03	EOSYFTRIP	EGDGK01ABET	%U3-SL	NR-AC2HR		
13	7.85E-09	6.90E-03	HSMPK00102	MXOPHDPLR	%U3-SL			
14	7.20E-09	6.30E-03	CVTKBRWT00	%U3-SL				
15	6.49E-09	5.70E-03	%U3-SL	FSDOW	FSOPH-V675	FSOPH-V676		
16	6.24E-09	5.50E-03	HSCVW20506	%U3-SL				
17	6.24E-09	5.50E-03	CVCVW30506	%U3-SL				
18	5.53E-09	4.80E-03	HCCQWHPP	MXOPHDPLR	%U3-SL			
19	5.46E-09	4.80E-03	HSMPW00102	MXOPHDPLR	%U3-SL			
20	5.31E-09	4.70E-03	%U3-SL	FSDIW	FSOPH-V675	FSOPH-V676		
21	5.26E-09	4.60E-03	%U3-SL	CWCUK1A1BD	CWCUW2A2BD			
22	5.05E-09	4.40E-03	HSCVWG540123	%U3-SL				
23	5.05E-09	4.40E-03	HSCVWG212347	%U3-SL				
24	4.53E-09	4.00E-03	HCCQMHPBP	HSMPM0001A	MXOPHDPLI	%U3-SL		
25	4.53E-09	4.00E-03	HSMPM0002B	HCCQMHPBP	MXOPHDPLI	%U3-SL		
26	3.22E-09	2.80E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWGCRCVCCF		
27	3.22E-09	2.80E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWLRCRCVCCF		
28	3.09E-09	2.70E-03	HSMPR0002B	HCCQMHPBP	MXOPHDPLI	%U3-SL		
29	3.09E-09	2.70E-03	HCCQMHPBP	HSMPR0001A	MXOPHDPLI	%U3-SL		
30	3.00E-09	2.60E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWSW2-LC		
31	3.00E-09	2.60E-03	%U3-SL	FSOPH-V675	FSOPH-V676	FSNWSW2-GC		
32	2.64E-09	2.30E-03	%U3-SL	CWCUK1A1BD	CWCUK2A2BD			
33	2.20E-09	1.90E-03	MXOPHDPLI	%U3-SL	FSDOW	FSOPH-HP02A	FSOPH-HP02B	
34	2.14E-09	1.90E-03	HSMPM0002B	HSMPR0001A	MXOPHDPLI	%U3-SL		
35	2.14E-09	1.90E-03	HSMPR0002B	HSMPM0001A	MXOPHDPLI	%U3-SL		
36	2.11E-09	1.80E-03	HSCVW42426	MXOPHDPLI	%U3-SL			
37	2.11E-09	1.80E-03	HSCVW40405	MXOPHDPLI	%U3-SL			
38	1.80E-09	1.60E-03	MXOPHDPLI	%U3-SL	FSDIW	FSOPH-HP02A	FSOPH-HP02B	
39	1.74E-09	1.50E-03	HCCQKHPP	MXOPHDPLR	%U3-SL			
40	1.72E-09	1.50E-03	HCCQMHPBP	HSMPM0001A	MXOPHDPLI	%U3-SL		

Table 5.8 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 1. for HR-SDN network communication

Value	F-V	BE #1	BE #2	BE #3	BE #4	BE #5
3.22E-09	1.61E-03	%U3-SL	FSNWLRCRVCCF	FSOPH-V675	FSOPH-V676	
3.22E-09	1.61E-03	%U3-SL	FSNWGCRCVCCF	FSOPH-V675	FSOPH-V676	
3.00E-09	1.50E-03	%U3-SL	FSNWSW2-GC	FSOPH-V675	FSOPH-V676	
3.00E-09	1.50E-03	%U3-SL	FSNWSW2-LC	FSOPH-V675	FSOPH-V676	
1.59E-09	7.94E-04	%U3-SL	FSNWGCTRSCCF	FSOPH-V675	FSOPH-V676	
1.47E-09	7.37E-04	%U3-SL	FSNWGCINTCCF	FSOPH-V675	FSOPH-V676	
1.47E-09	7.37E-04	%U3-SL	FSNWLCONTCCF	FSOPH-V675	FSOPH-V676	
1.09E-09	5.44E-04	%U3-SL	FSNWLRCRVCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.09E-09	5.44E-04	%U3-SL	FSNWGCRCVCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.01E-09	5.07E-04	%U3-SL	FSNWSW2-GC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.01E-09	5.07E-04	%U3-SL	FSNWSW2-LC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
5.37E-10	2.68E-04	%U3-SL	FSNWGCTRSCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
4.98E-10	2.49E-04	%U3-SL	FSNWGCINTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
4.98E-10	2.49E-04	%U3-SL	FSNWLCONTCCF	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
3.00E-10	1.50E-04	%U3-SL	FSNWSW-LC	FSOPH-V675	FSOPH-V676	
3.00E-10	1.50E-04	%U3-SL	FSNWSW-GC	FSOPH-V675	FSOPH-V676	
1.29E-10	6.40E-05	%U3-SL	FSNWLRCRVCCF	FSOPH-V675	HSMVO0676B	
1.29E-10	6.40E-05	%U3-SL	FSNWLRCRVCCF	FSOPH-V676	HSMVO0675A	
1.29E-10	6.40E-05	%U3-SL	FSNWGCRCVCCF	FSOPH-V675	HSMVO0676B	
1.29E-10	6.40E-05	%U3-SL	FSNWGCRCVCCF	FSOPH-V676	HSMVO0675A	
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-GC	FSOPH-V676	HSMVO0675A	
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-GC	FSOPH-V675	HSMVO0676B	
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-LC	FSOPH-V676	HSMVO0675A	
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-LC	FSOPH-V675	HSMVO0676B	
1.01E-10	5.10E-05	%U3-SL	FSNWSW-LC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.01E-10	5.10E-05	%U3-SL	FSNWSW-GC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI

Table 5.9 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 2. for HR-SDN network communication

Value	F-V	BE #1	BE #2	BE #3	BE #4	BE #5
3.00E-09	1.51E-03	%U3-SL	FSNWSW2-LC	FSOPH-V675	FSOPH-V676	
3.00E-09	1.51E-03	%U3-SL	FSNWSW2-GC	FSOPH-V675	FSOPH-V676	
1.01E-09	5.10E-04	%U3-SL	FSNWSW2-LC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.01E-09	5.10E-04	%U3-SL	FSNWSW2-GC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
3.00E-10	1.51E-04	%U3-SL	FSNWSW-LC	FSOPH-V675	FSOPH-V676	
3.00E-10	1.51E-04	%U3-SL	FSNWSW-GC	FSOPH-V675	FSOPH-V676	
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-LC	FSOPH-V676	HSMVO0675A	
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-LC	FSOPH-V675	HSMVO0676B	
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-GC	FSOPH-V675	HSMVO0676B	
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-GC	FSOPH-V676	HSMVO0675A	
1.01E-10	5.10E-05	%U3-SL	FSNWSW-LC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
1.01E-10	5.10E-05	%U3-SL	FSNWSW-GC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-LC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLR
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-LC	FSOPH-HP02A	FSOPH-V676	MXOPHDPLR
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-LC	FSOPH-HP02B	FSOPH-V675	MXOPHDPLR
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-GC	FSOPH-HP02B	FSOPH-V675	MXOPHDPLR
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-GC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLR
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-GC	FSOPH-HP02A	FSOPH-V676	MXOPHDPLR
3.53E-11	1.80E-05	%U3-SL	FSNWGCRCVCCF	FSOPH-V675	FSOPH-V676	
3.53E-11	1.80E-05	%U3-SL	FSNWLRCVCCF	FSOPH-V675	FSOPH-V676	

Table 5.10 Dominant MCSs related to network failure of IE SLOCA CD sequences in case 3. for HR-SDN network communication

Value	F-V	BE #1	BE #2	BE #3	BE #4	BE #5	BE #6
3.00E-09	1.51E-03	%U3-SL	FSNWSW2-GC	FSOPH-V675	FSOPH-V676		
3.00E-09	1.51E-03	%U3-SL	FSNWSW2-LC	FSOPH-V675	FSOPH-V676		
1.01E-09	5.10E-04	%U3-SL	FSNWSW2-GC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI	
1.01E-09	5.10E-04	%U3-SL	FSNWSW2-LC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI	
3.00E-10	1.51E-04	%U3-SL	FSNWSW-LC	FSOPH-V675	FSOPH-V676		
3.00E-10	1.51E-04	%U3-SL	FSNWSW-GC	FSOPH-V675	FSOPH-V676		
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-GC	FSOPH-V676	HSMVO0675A		
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-GC	FSOPH-V675	HSMVO0676B		
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-LC	FSOPH-V675	HSMVO0676B		
1.20E-10	6.00E-05	%U3-SL	FSNWSW2-LC	FSOPH-V676	HSMVO0675A		
1.01E-10	5.10E-05	%U3-SL	FSNWSW-LC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI	
1.01E-10	5.10E-05	%U3-SL	FSNWSW-GC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLI	
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-GC	FSOPH-HP02A	FSOPH-V676	MXOPHDPLR	
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-GC	FSOPH-HP02B	FSOPH-V675	MXOPHDPLR	
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-GC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLR	
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-LC	FSOPH-HP02A	FSOPH-HP02B	MXOPHDPLR	
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-LC	FSOPH-HP02B	FSOPH-V675	MXOPHDPLR	
9.21E-11	4.60E-05	%U3-SL	FSNWSW2-LC	FSOPH-HP02A	FSOPH-V676	MXOPHDPLR	
3.00E-11	1.50E-05	%U3-SL	FSNWSW2-GC	FSOPH-HP02A	FSOPH-HP02B	FSOPH-LP01A	FSOPH-LP01B
3.00E-11	1.50E-05	%U3-SL	FSNWSW2-LC	FSOPH-HP02A	FSOPH-HP02B	FSOPH-LP01A	FSOPH-LP01B

Table 5.11 Summary of the risk quantification results
for HR-SDL network communication

Description	Case 1.	Case 2.	Case 3.
Software failure probability	1.00E-04	1.00E-04	1.00E-04
Periodic inspection interval	730 hours	8 hours	50 ms
Failure of hardware components in NW module (IFM, RxM, TxM of GC/LC) [①]	1.01E-07	1.10E-09	2.01E-15
Failure of software in GC/LC [②]	8.03E-10	8.03E-10	8.03E-10
Top event (Small LOCA CD sequences) [③]	1.23E-06	1.12E-06	1.12E-06
Risk contribution of network failure ([①+②]/ ③)	8.28%	0.17%	0.07%

Table 5.12 Summary of the risk quantification results
for HR-SDN network communication

Description	Case 1.	Case 2.	Case 3.
Software failure probability (Network module in GC/LC)	1.00E-04	1.00E-04	1.00E-04
Software failure probability (Application software in GC/LC)	1.00E-03	1.00E-03	1.00E-03
Periodic inspection interval	730 hours	8 hours	50 ms
Failure of hardware components in NW module (IFM, RxM, TxM of GC/LC) [①]	1.72E-08	1.88E-10	2.60E-16
Failure of software in GC/LC [②]	1.03E-08	1.03E-08	1.03E-08
Top event (Small LOCA CD sequences) [③]	1.14E-06	1.13E-06	1.13E-06
Risk contribution of network failure ([①+②]/③)	2.41%	0.93%	0.92%

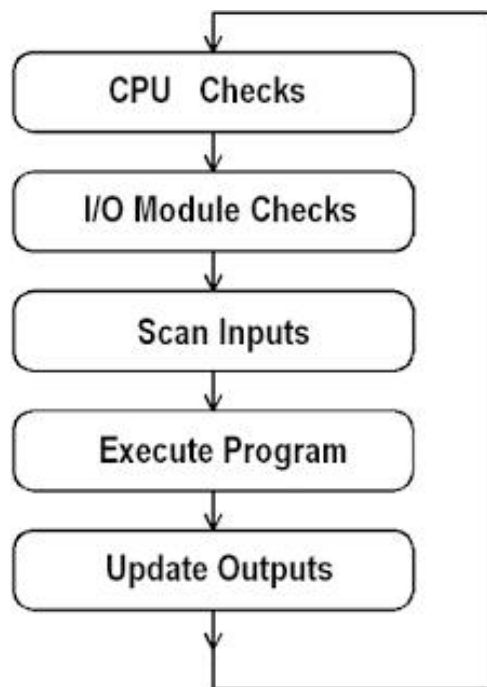


Figure 5.1 General cycle of PLC self-diagnostics

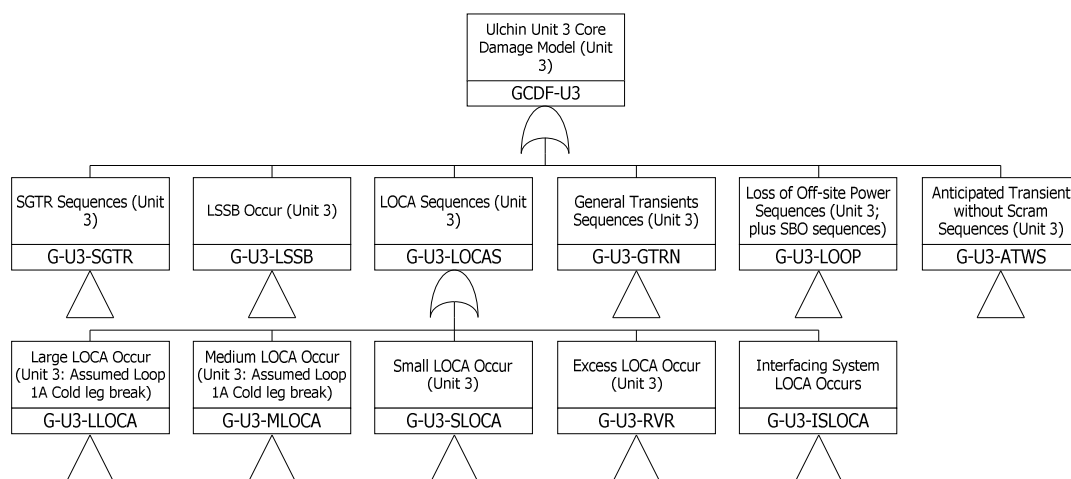


Figure 5.2 One-top fault-tree model for OPR-1000 nuclear power plant

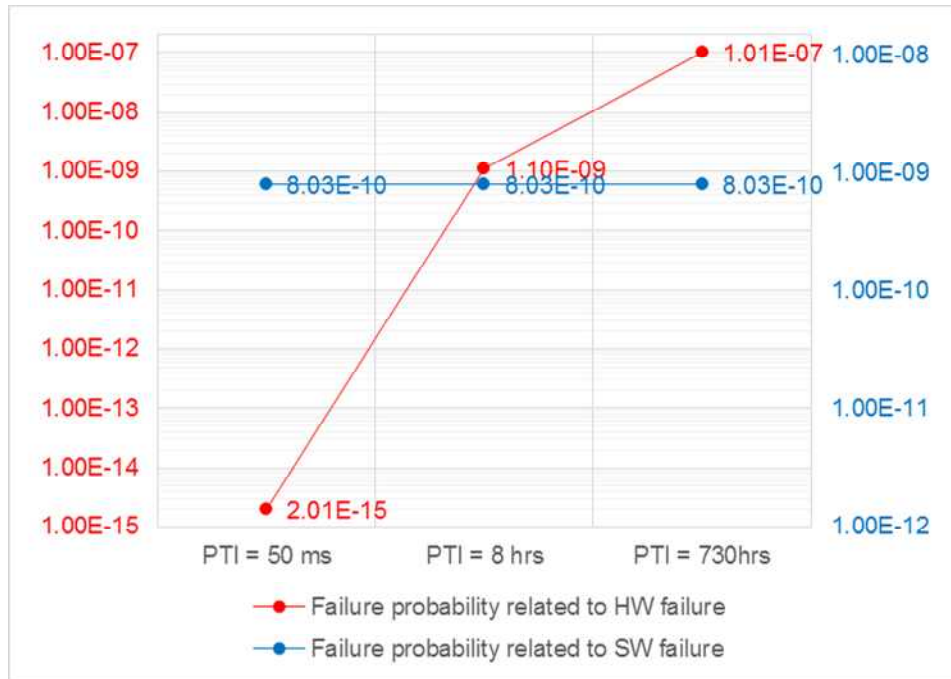


Figure 5.3 Sensitivity study results for the effect of periodic test interval on network failure in case of HR-SDL network communication

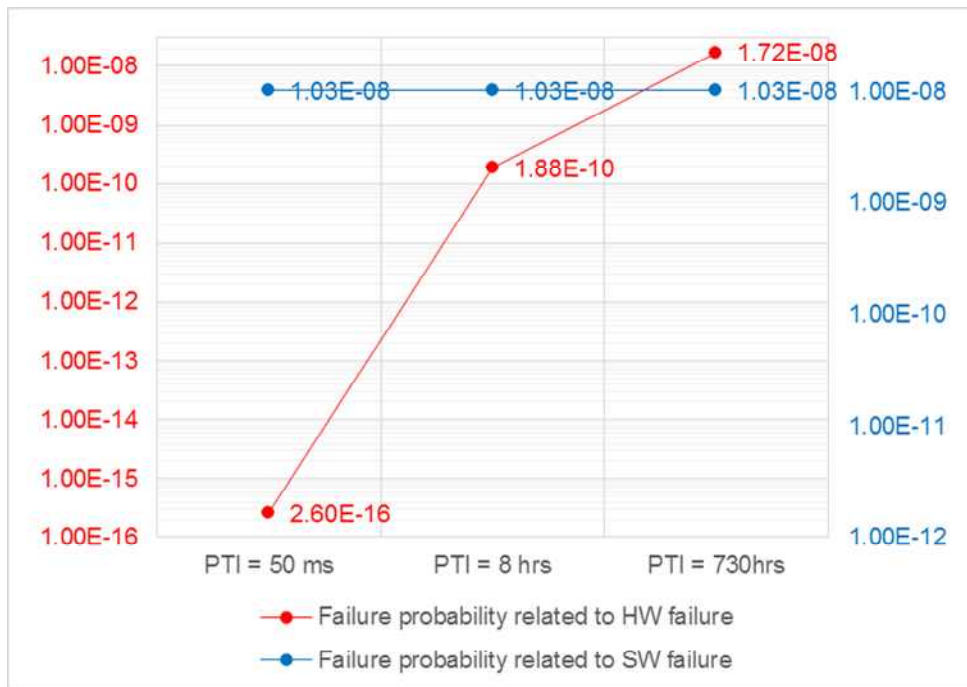


Figure 5.4 Sensitivity study results for the effect of periodic test interval on network failure in case of HR-SDL network communication

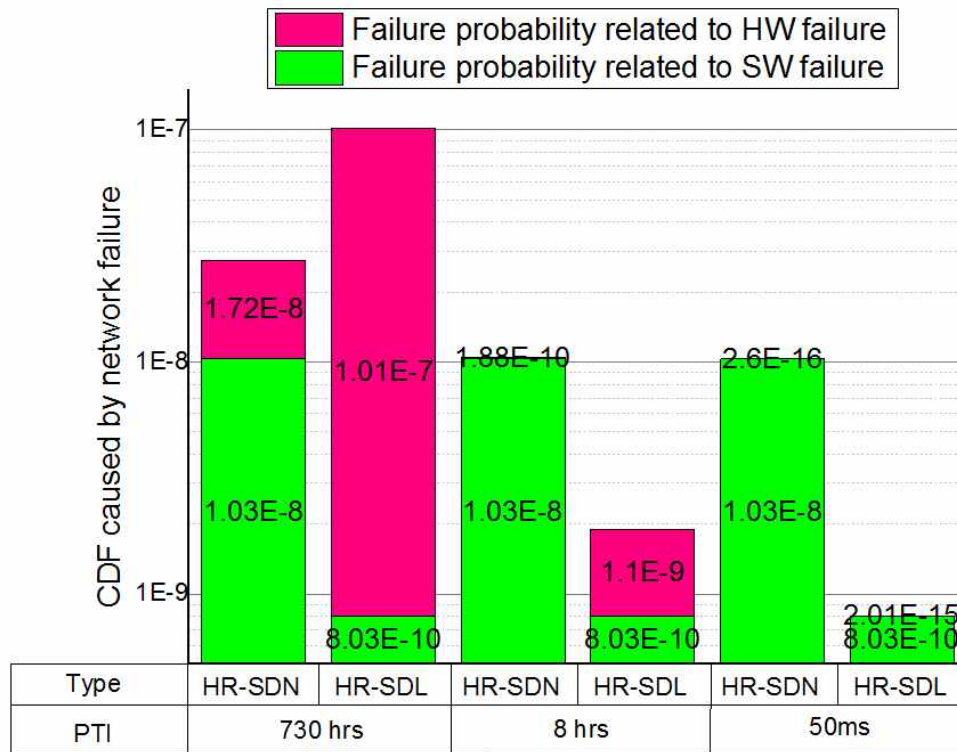


Figure 5.5 Summary of sensitivity study results on various periodic test interval

Chapter 6. Conclusion

ESF-CCS, which employs a network communication system for the transmission of safety-critical information from the GCs to the LCs, was developed to effectively accommodate a vast number of field controllers. However, the application of the developed ESF-CCS in NPPs has faced challenges regarding the regulatory requirements of safety-related digital systems because the risk effects of network communication failure on the overall plant risk have not yet been completely quantified. Therefore, a framework for identifying the potential hazardous states of network communication in the ESF-CCS and quantifying the corresponding causes was proposed, and a fault-tree model for network communication failure was developed to estimate the risk effects of network failure between the GCs and LCs on ESF-CCS signal failure; the developed fault-tree model was then applied to several case studies.

Based on the general operational characteristics of the Profibus protocol, which includes four major processes: token frame reception, data frame transmission, data frame reception and token frame passing, the hazard states for network communication between GCs and LCs were identified in both protocol level. The failure of automatic signal generation by LC in ESF-CCS for the field component actuation in ESFAS condition, which is the top hazardous state considering the main function of ESF-CCS, can be caused by a failure of LC input generation by GC, including failure of token reception, data transmission, and token reception by GC, and data reception by LC. Since the diversity concept is implemented in ESF-CCS to ensure reliable data communication, the hazardous states in system level can be structured in detailed considering the redundant structure of GCs, LCs, and network bus in ESF-CCS. According to the identified hazardous states, the failure mechanisms of network communication were identified based on the OSI layer

structure of general Profibus protocol. For the defined independent three layers in Profibus protocol: Physical layer, Data Link layer, and Application layer, the failure mechanisms of network communication include: failure of the hardware components of the network module, failure of the software to perform the intended function, and failure due to medium-related bit errors, where each failure may result in a failure to generate ESF actuation signal in ESFAS condition. In addition, the quantification scheme for each failure cause is proposed in this study.

In this study, a fault-tree model of GC-LC network communication failure was developed and integrated with OPR-1000 PSA model, based on the redundancy concept as well as the identified hazardous states and corresponding causes of failure regarding network communication between GCs and LCs. Based on the developed fault-tree model for HR-SDL and HR-SDN network communication, the MCSs for initiating event SLOCA which include basic events related to network failure were identified. As a sensitivity study, three case studies were performed based on the periodic test methods for hardware components in GC and LC network module and their test intervals in this study. Three case studies include the manual testing, automatic testing by ETIP, and automatic testing by PLC scan of GC and LC network modules. Based on the cutset analysis result, the dominant cut sets for ESF-CCS signal failure include the CCF of both hardware components or modules and software implemented in GC and LC.

In terms of risk effect of network failure on the SLOCA CD sequences, overall risk of network communication failure between GC and LC in ESF-CCS contributed up to 8.28% to the ESF component actuation signal failure, while network risk contributed up to 2.41% to the ESF component actuation signal failure, when manual testing for network hardware components were assumed. The quantification results for both network protocol applied in network communication between GC and LC in ESF-CCS reveal the potential application of HR-SDN network communication in NPP protection system compared to the conventional

point-to-point data exchanging method such as HR-SDL network communication in terms of reliability. Considering the conventional testing of the modules in NPP protection systems, such as RPS and ESF-CCS; that is, manual periodic testing with the interval of 730 hours, application of HR-SDN for safety-critical signal exchange between GC and LC in ESF-CCS has the advantage in terms of reliability of the system, compared to the case of HR-SDL system. This was because of high dependency of hardware component or module failure in Data Link layer for the case of HR-SDL network protocol, compared to the case of HR-SDN network protocol.

This study is expected to provide insight into the development of the fault-tree model for the network failure in digital I&C system and into the quantification of the risk effect of network failure for safety-critical information transmission in NPPs. As a further study, the risk effects of network failure in the ESF-CCS on the CDF can be estimated in a more detailed manner by analyzing the failure modes and failure causes, in a sub-component level by means of failure mode and effects analysis (FMEA) and the fault detection coverage (FDC) of the fault tolerance techniques (FTTs) for the associated hazardous states after the detailed configuration of ESF-CCS is decided [90]. Based on the module-specific FMEA, the unavailability of the hardware components can be optimistically estimated by considering the estimated FDC of the FTTs and test interval for both manual testing and self-diagnostics. In addition, the relationship among the human action failures must be investigated to consider multiple human error condition since ESF-CCS provides multiple manual actuation to assure the diversity of the system. Since the conventional HEP method cannot accommodate the multiple conditions in a fault tree, condition-based human reliability assessment method can be applied to include a complex relationship among the automated safety signal generation and the human operator's manual actuation, avoiding the optimistic estimation of HEP of the human action failure [91].

References

- [1] National Research Council. (1997). Digital Instrumentation and Control Systems in Nuclear Power Plants: safety and reliability issues, National Academy Press, DC, USA.
- [2] Kisner, R., Mullens, J., Wilson, T., Wood, R., Korsah, K., Qualls, A., ... & Loebl, A. (2007). Safety and Nonsafety Communications and Interactions in International Nuclear Power Plants. Oak Ridge National Laboratory, United States.
- [3] International Electrotechnical Commission. (1999). IEC 61375-1. Train Communication Network.
- [4] IEEE power engineering society (2009). IEEE Std.603-2009. IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,.
- [5] IEEE power engineering society (1993). IEEE Std. 7-4.3.2-2010. IEEE standard criteria for digital computers in safety systems of nuclear power generating station.
- [6] Aldemir, T., Miller, D. W., Stovsky, M., Kirschenbaum, J., Bucci, P., Mangan, L. A., ... & Arndt, S. A. (2007). Methodologies for the probabilistic risk assessment of digital reactor protection and control systems. Nuclear technology, 159(2), 167-191.
- [7] Kang, H. G., Kim, M. C., Lee, S. J., Lee, H. J., Eom, H. S., Choi, J. G., & Jang, S. C. (2009). An overview of risk quantification issues for digitalized nuclear power plants using a static fault tree. Nuclear Engineering and Technology, 41(6), 849-858.
- [8] Lee, Dong-Young, et al (2008). "Development experience of digital safety system in Korea." IAEA Technical Meeting on the impact of Digital I&C Technology on the Operation and Licensing of NPP, Beijing, China, 2008.
- [9] J.-P. Burel, F. Dalik, K. Wagner, Miroslav RIS, and J.-P. Mauduit (2002). NEA/CSNI/R(2002)1/Vol. 2. Modernization of I&C systems for the ANP Dukovany by the use of computer-based equipment.

- [10] Kisner, R. A. (2009). Design Practices for Communications and Workstations in Highly Integrated Control Rooms. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.
- [11] K. Burak (2006). "Ethernet Redundancy." ANS 5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface, Albuquerque, New Mexico, November 12 - 16, 2006.
- [12] L. Meter (2006). "Invensys Solution for a Complete Digital I&C System Upgrade for a Nuclear Power Plant." ANS 5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface, Albuquerque, New Mexico, November 12 - 16, 2006.
- [13] Haugdahl, J. Scott. Network analysis and troubleshooting, Addison-Wesley Professional, 2000.
- [14] J. A. Lenner (2003). "The Development of Safety Networks in a 61508 Environment." ISA Expo 2003.
- [15] International Electro technical Commission. IEC 61784-3/CDV, Digital Data Communications for Measurement and Control - draft version 4.0.
- [16] Stallings, W. (2007). Data and computer communications. Pearson/Prentice Hall.
- [17] Aldemir, T. (2006). Current state of reliability modeling methodologies for digital systems and their acceptance criteria for nuclear power plant assessments, US Nuclear Regulatory Commission.
- [18] Dugan, J. B., Bavuso, S. J., & Boyd, M. A. (1993). Fault trees and Markov models for reliability analysis of fault-tolerant digital systems. Reliability Engineering & System Safety, 39(3), 291-307.
- [19] Bucci, P., Kirschenbaum, J., Mangan, L. A., Aldemir, T., Smith, C., & Wood, T. (2008). Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. Reliability Engineering & System Safety, 93(11), 1616-1627.
- [20] Kang, H. G., & Jang, S. C. (2008). A quantitative study on risk issues in safety feature control system design in digitalized nuclear power plant. Journal of nuclear science and technology, 45(8), 850-858.
- [21] Gustafsson, Johan (2012). Reliability analysis of safety-related digital instrumentation and control in a nuclear power plant, Royal Institute of Technology.
- [22] Smith, D. T., Delong, T. A., & Johnson, B. W. (2000). A Safety

Assessment Methodology for Complex Safety-Critical Hardware/Software Systems. Proc. Int. Topl. Mtg. Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies, 13-16.

[23] Jian, S., & Shaoping, W. (2006, December). Reliability analysis and congestion control on network nodes. In Robotics, Automation and Mechatronics, 2006 IEEE Conference on (pp. 1-6). IEEE.

[24] Ajmone Marsan, M., Conte, G., & Balbo, G. (1984). A class of generalized stochastic Petri nets for the performance evaluation of multiprocessor systems. ACM Transactions on Computer Systems (TOCS), 2(2), 93-122.

[25] Lu, L., & Jiang, J. (2004). Probabilistic safety assessment for instrumentation and control systems in nuclear power plants: an overview. Journal of nuclear science and technology, 41(3), 323-330.

[26] Chi T. L. (2008). Traditional probabilistic risk assessment methods for digital systems. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research.

[27] IAEA (2009). IAEA Nuclear Energy Series NP-T-1.5, Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants.

[28] Chu, T.L. (2013). Development of quantitative software reliability models for digital protection systems of nuclear power plants. US Nuclear Regulatory Commission.

[29] Brazendale, J. (1995, August). IEC 1508: Functional Safety: Safety-Related Systems. In Software Engineering Standards Symposium, 1995.(ISESS 95 'Experience and Practice', Proceedings., Second IEEE International (pp. 8-17). IEEE.

[30] Bäckström, O., et al. (2014). "Quantification of reactor protection system software reliability based on indirect and direct evidence." Probabilistic Safety Assessment and Management (PSAM 12), June 2014, Honolulu, Hawaii.

[31] Leveson, N. G. (1995). Safeware: system safety and computers. ACM.

[32] Preckshot, G. G. (1993). Data communications (No. NUREG/CR--6082; UCRL-ID--114567). Nuclear Regulatory Commission, Washington, DC (United States). Div. of Reactor Controls and Human Factors; Lawrence Livermore National Lab., CA (United States).

- [33] Hong, S. H., & Kim, K. A. (1997). Implementation and performance evaluation of Profibus in the automation systems. In *Factory Communication Systems, 1997. Proceedings. 1997 IEEE International Workshop on* (pp. 187-192). IEEE.
- [34] Tovar, E., & Vasques, F. (1999). Real-time fieldbus communications using Profibus networks. *Industrial Electronics, IEEE Transactions on*, 46(6), 1241-1251.
- [35] Vitturi, S. (2004). On the effects of the acyclic traffic on Profibus DP networks. *Computer Standards & Interfaces*, 26(2), 131-144.
- [36] Vitturi, S. (2004). Stochastic model of the Profibus DP cycle time. *IEE Proceedings-Science, Measurement and Technology*, 151(5), 335-342.
- [37] Willig, A., & Wolisz, A. (2001). Ring stability of the PROFIBUS token-passing protocol over error-prone links. *Industrial Electronics, IEEE Transactions on*, 48(5), 1025-1033.
- [38] Jung, H. G., & Seong, P. H. (2001). Fault-tolerance performance evaluation of fieldbus for NPCS network of KNGR. *Nuclear Engineering and Technology*, 33(1), 1-11.
- [39] Carvalho, J. A., Carvalho, A. S., & Portugal, P. J. (2005, September). Assessment of PROFIBUS networks using a fault injection framework. In *Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on* (Vol. 1, pp. 9-pp). IEEE.
- [40] Carvalho, J. A., Carvalho, A. S., & Portugal, P. J. (2005, November). Experimental analysis of outage times for PROFIBUS network. In *Industrial Electronics Society, 2005. IECON 2005. 31st Annual Conference of IEEE* (pp. 6-pp). IEEE.
- [41] Cavalieri, S., Monforte, S., Tovar, E., & Vasques, F. (2002, August). Evaluating worst case response time in mono and multi-master Profibus DP. In *4th IEEE International Workshop on Factory Communication Systems* (pp. 233-240).
- [42] Kang, H. G., & Jang, S. C. (2008). A quantitative study on risk issues in safety feature control system design in digitalized nuclear power plant. *Journal of nuclear science and technology*, 45(8), 850-858.
- [43] Al-Dabbagh, A. W., & Lu, L. (2010). Design and reliability assessment of control systems for a nuclear-based hydrogen production plant with copper - chlorine thermochemical cycle. *International journal of*

hydrogen energy, 35(3), 966-977.

[44] Zurawski, R., & Zhou, M. (1994). Petri nets and industrial applications: A tutorial. *Industrial Electronics, IEEE Transactions on*, 41(6), 567-583.

[45] Liu, T. S., & Chiou, S. B. (1997). The application of Petri nets to failure analysis. *Reliability Engineering & System Safety*, 57(2), 129-142.

[46] Labeau, P. E., Smidts, C., & Swaminathan, S. (2000). Dynamic reliability: towards an integrated platform for probabilistic risk assessment. *Reliability Engineering & System Safety*, 68(3), 219-254.

[47] Kwon, K. C., & Lee, M. (2009). Technical review on the localized digital instrumentation and control systems. *Nuclear engineering and technology*, 41(4), 447-454.

[48] Korea Electric Power Corporation & Korea Hydro & Nuclear Power Co., Ltd (2013). APR1400-Z-J-EC-13001-NP Rev.0, Safety I&C System for the APR1400

[49] Kim, C. H., Lee, D. Y., & Park, H. S. (2007). "Performance Analysis and Test Results of a High Reliability-Safety Data Link (HR-SDL) for a Safety Grade PLC (POSAFE-Q)." *Transactions of the Korean Nuclear Society Spring Meeting*, May 10-11, 2007, Jeju, Korea.

[50] Shekhawat R S (1997). Design and Implementation of PROFIBUS FDL-Internal Report-Ver. 1.

[51] Verwer Training and Consultancy Ltd. (2013). PROFIBUS Installation Guidelines-Rev. 11.2.

[52] Kim, Young Jin, et al (2008). Design Support for ESF-CCS. Korea Atomic Energy Research Institute, Daejeon, Republic of Korea.

[53] Kim, Seong Tae, et al (2006). "New Design of Engineered Safety Features-component Control System to Improve Performance and Reliability." *PBNC 2006*, Sydney, Australia, pp. 489.

[54] Willig, A. (2003). Polling-based MAC protocols for improving real-time performance in a wireless PROFIBUS. *Industrial Electronics, IEEE Transactions on*, 50(4), 806-817.

[55] IEEE (1985). IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification, IEEE, New York, USA.

[56] Tovar, E., & Vasques, F. (1999). Real-time fieldbus communications

using Profibus networks. *Industrial Electronics, IEEE Transactions on*, 46(6), 1241-1251.

[57] Siemens (1997). SIMATIC NET ASPC 2 / Hardware User Description. Siemens AG, Germany

[58] Felser, M. (2002). The fieldbus standards: History and structures." University of Applied Science Berne.

[59] Kang, H. G. (2009). Issues in System Reliability and Risk Model. In *Reliability and Risk Issues in Large Scale Safety-critical Digital Control Systems* (pp. 25-46). Springer London.

[60] IEEE (2011). IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification, IEEE, New York, USA.

[61] Haugdahl, J. Scott. Network analysis and troubleshooting. Addison-Wesley Professional, 2000.

[62] IEC (2014). IEC 61158-2:2014, Industrial communication networks - Fieldbus specifications - Part 2: Physical layer specification and service definition, IEC.

[63] Jeruchim, M. C. (1984). Techniques for estimating the bit error rate in the simulation of digital communication systems. *Selected Areas in Communications, IEEE Journal on*, 2(1), 153-170.

[64] Mackay, S. (2004). Practical industrial data networks: design, installation and troubleshooting. Newnes.

[65] IEC (2010). IEC 61158-5-10:2010, Industrial communication networks - Fieldbus specifications - Part 5-10: Application layer service definition - Type 10 elements, IEC.

[66] Koo, S. R., & Seong, P. H. (2006). Software design specification and analysis technique (SDSAT) for the development of safety-critical systems based on a programmable logic controller (PLC). *Reliability Engineering & System Safety*, 91(6), 648-664.

[67] Lee, MyeongKyun, SeungWhan Song, and DongHwa Yun (2012). "Development and Application of POSAFE-Q PLC Platform, IAEA.

[68] Hur, S., Kim, D. H., Choi, J. K., Park, J. C., Seong, S. H., & Lee, D. Y. (2006). Reliability analysis and component functional allocations for the ESF multi-loop controller design. In *Reliability, safety and hazard: advances in risk-informed technology*.

- [69] KyungChul, Choi, et al (2007). "Design of High Reliable Safety Data Link (HR-SDL) for Safety Grade PLC (POSAFE-Q) for Nuclear Power Plants." Proceedings of the 17th World Congress The International Federation of Automatic Control, pp. 126-128.
- [70] Lee Dong Young, et al (2008). KAERI/RR-2914/2007, Development of the Digital Reactor Safety System, Daejeon, Republic of Korea: Korea Atomic Energy Research Institute.
- [71] Chu, T. L., et al. (2009). Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods, US Nuclear Regulatory Commission.
- [72] Quanterion Solutions Inc (2008). Photonic Component and Subsystem Reliability Process Final Report, Penn State University Electro-Optics Center, PA, USA.
- [73] Ohring, Milton (1998). Reliability and failure of electronic materials and devices. Academic Press.
- [74] Maher, J. Michael (1989). "Real-Time Control and Communications." 18th Annual ESD/SMI International Programmable Controllers Conference Proceedings, 1989.
- [75] Brown, S. (2000). Overview of IEC 61508. Design of electrical/electronic/programmable electronic safety-related systems. Computing & Control Engineering Journal, 11(1), 6-12.
- [76] IEEE Computer Society (2005). IEEE Std 1012TM-2004, IEEE Standard for Software Verification and Validation, IEEE.
- [77] Schäfer M. (1998). "New concepts for safety-related bus systems", 3rd International Symposium "Programmable Electronic Systems in Safety Related Applications, 1998.
- [78] Irwin, J. David (1997). The industrial electronics handbook. CRC Press.
- [79] Acromag Incorporated (2002). BusWorks 900 PB Series ProfiBus/RS485 Network I/O Modules Technical Reference, Introduction to ProfiBus DP, Acromag Incorporated, MI, USA.
- [80] Poloski J. P. (2000), NUREG/CR-5500 Vol. 9, Reliability Study: High-Pressure Safety Injection System, US Nuclear Regulatory Commission.
- [81] Kessler, Günter, et al (2014). The Risks of Nuclear Energy Technology: Safety Concepts of Light Water Reactors. Springer.

- [82] Casada, D. A. (1990). Auxiliary feedwater system aging study (No. NUREG/CR-5404-Vol. 1; ORNL--6566/V1). Nuclear Regulatory Commission, Washington, DC (USA). Div. of Engineering; Oak Ridge National Lab., TN (USA).
- [83] IAEA (2004). Safety guide NS-G-1.10, Design of Reactor Containment Systems for Nuclear Power Plants, IAEA.
- [84] IAEA (1990). NPX80-ICDP640-01, Design Procedure for Component Control System Component Functional Grouping for NUPLEX 80+, IAEA.
- [85] Hur, Seop, et al (2006). "Component Functional Allocations of the ESF Multi-loop Controller for the KNICS ESF-CCS Design.", Transactions of the Korean Nuclear Society Spring Meeting, 2006, Chuncheon, Korea.
- [86] Heising, C. D., & Guey, C. N. (1984). A comparison of methods for calculating system unavailability due to common cause failures: the beta factor and multiple dependent failure fraction methods. Reliability Engineering, 8(2), 101-116.
- [87] EPRI (2012). Modeling of Digital Instrumentation and Control in Nuclear Power Plant Probabilistic Risk Assessments, EPRI.
- [88] Enzinna, B., Shi, L., & Yang, S. (2009, April). Software common-cause failure probability assessment. In Sixth American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC&HMIT, pp. 5-9.
- [89] Choi, J. G., Lee, S. J., Kang, H. G., Hur, S., Lee, Y. J., & Jang, S. C. (2012). Fault detection coverage quantification of automatic test functions of digital I&C system in NPPS. Nuclear Engineering and Technology, 44(4), 421-428.
- [90] Lee, S. J., Choi, J. G., Kang, H. G., & Jang, S. C. (2010). Reliability assessment method for NPP digital I&C systems considering the effect of automatic periodic tests. Annals of Nuclear Energy, 37(11), 1527-1533.
- [91] Kang, H. G., & Jang, S. C. (2006). Application of condition-based HRA method for a manual actuation of the safety features in a nuclear power plant. Reliability Engineering & System Safety, 91(6), 627-633.

요 약 문

원자력 발전소에 적용된 안전 등급 네트워크 통신망의 신뢰도 평가에 관한 연구

최근, 원자력 발전소 내 공학적 안전설비 작동을 위한 그룹제어기와 루프제어기 간의 안전 신호의 송수신을 위해, 네트워크 통신망이 적용된 공학적 안전설비-기기 제어계통 (ESF-CCS)가 개발되었다. 원자력 발전소 내의 시스템의 제어나 정보 전달 계통 등에 네트워크 통신망을 이용할 경우, 설계상의 유연성 및 비용 절감 등의 면에서 많은 장점이 있지만, ESF-CCS내 네트워크 통신망에 대한 리스크 영향 평가 방법이 정립되어 있지 않고, 네트워크 통신 실패가 원전 리스크에 미치는 영향이 평가되어 있지 않아, 실제로 발전소에 적용되지 못하고 있다.

따라서, 본 연구에서는 ESF-CCS내의 그룹제어기와 루프제어기간의 데이터 송수신에 적용된 고신뢰도 안전데이터링크 (HR-SDL)와 고신뢰도 안전데이터망 (HR-SDN)의 위해상태 및 실패기제들을 분석하였다. 이를 바탕으로, 네트워크 통신 실패로 인한 공학적 안전 설비 (ESF) 작동 실패의 고장수목을 모델링하고, 원전 PSA 모델에 반영하여, 네트워크 통신 실패의 리스크 영향을 정량적으로 분석하였다.

네트워크 통신망의 위해상태를 분석하기 위해서, HR-SDL과 HR-SDN의 네트워크 프로토콜인 프로피버스 (Profibus) 프로토콜의 통신 방법에 근거하여, 그룹제어기와 루프제어기의 위해상태를 정의하였다. 정의된 위해상태들을 초래할 수 있는 실패기제를 분석하기 위해, Profibus에서 정의된 3가지 OSI 계층 (물리 계층, 데이터 링크 계층, 응용 계층)에 해당하는 실패기제들을 분석하였다. 분석된 실패기제들은 크게 하드웨어 실패, 소프트웨어 실패, 송수신되는 프레임 내의 비트 오류발생으로 인한 실패로 분류되며, 각 실패기제에 대한 정량화 방안을 제안하였다.

제안된 방법론을 바탕으로, 원전의 DBA 사고 시, 공학적 안전신호를 필요로 하는 공학적 안전설비 작동 실패에 대한 고장수목 모델링을 수행하였다. 개발된 고장수목 모델을 한국 표준형 원전의 확률론적 안전성 평가 모델에 반영하여, ESF-CCS내 그룹제어기와 루프제어기간의 네트워크 통신 실패가 ESF 개시신호 생성 실패에 미치는 영향을 정량적으로 분석하였다. 본 연구의 제안된 방법론은 다른 디지털 계측제어 계통 내 안전 네트워크 통신망에 대한 리스크 평가에도 활용될 것으로 기대된다.

핵심어: 원자력 발전소; 디지털 계측제어 계통; 안전 등급 네트워크 통신망; 고장수목 모델링

감 사 의 글

제 2년간의 석사과정에 도움을 주신 많은 분들께 감사의 마음을 담아 이 글을 적습니다. 먼저, 저를 지도해주신 강현국 교수님께 깊은 감사를 드리고 싶습니다. 연구방향을 설정해주시고, 연구에 대한 조언을 아끼지 않고 해주신 강현국 교수님, 진심으로 감사드립니다. 앞으로 박사과정에서도, 교수님의 가르침에 따라 최선을 다해 좋은 연구를 할 수 있도록 노력하겠습니다. 그리고 본 연구의 심사를 수락해주시고, 더욱 가치 있는 연구가 될 수 있도록 아낌없는 조언을 주신 성풍현 교수님, 임춘택 교수님께도 감사의 말씀을 전합니다. 또한, 연구 진행에 있어서 많은 도움을 주시고 조언해주신 이승준 교수님께도 깊은 감사의 말씀을 올립니다.

석사생활 중 대부분의 시간을 함께 보냈던 연구실 선배님, 후배님들께도 감사의 말씀을 드립니다. 연구에 대해 많은 도움을 주심과 함께, 화목한 연구실 생활을 제공해주신 연구실 선배님들 덕분에 행복하고 유익한 2년이 될 수 있었습니다. 특히, 연구뿐만 아니라 대학원생이 가져야 할 인성과 예절을 가르쳐주신 신성민 선배님, 연구실 신입생 때 랩장으로서 연구실 생활에 대해 지도해주신 김보경 선배님, 연구 진행에 있어서 많은 도움과 아이디어를 주신 김희은 선배님, 현 랩장으로서 대학원 생활에 대해 많은 것을 알려주시고 화목한 연구실 생활이 되도록 도와주신 전인섭 선배님, 바쁘신 와중에도 연구실 생활을 많이 도와주신 함재현 선배님, 연구에 대해 많은 조언을 주신 Robby and Belal 선배님, 연구실 생활뿐만 아니라 사회구성원으로서 가져야 할 예절에 대해 많은 조언을 해주신 강길범 선배님, 학부 선배님으로서 연구실 생활에 잘 적응할 수 있도록 도와주신 유민 선배님, 화목한 연구실 생활이 되도록 도와주신 김지희 선배님께 감사의 말씀을 올립니다. 또한, 연구실 일이 있을 때마다 물심양면으로 도움을 준 이인효 후배님, 윤미래 후배님, 이동규 후배님, 연구 외적인 부분에서 많은 도움을 주신 김지숙 사무원님께 감사의 말씀을 전합니다.

마지막으로, 석사과정 동안 저를 물심양면으로 도와주시고 지원해주신 부모님과 가족들에게 감사의 말을 전합니다. 또한, 공부하는 동안 항상 옆에서 응원해주고 힘이 되어준 여자친구 황미리에게도 감사의 말을 전합니다. 그 외에도, 제 2년간의 석사생활 동안 함께 해주신 모든 분들께, 다시 한 번 감사드립니다.

이 력 서

성 명: 이 상 훈

생년월일: 1991. 07. 01

학 력

2007-2010 Goyang Foreign Language High School

2010-2014 B.S., Department of Nuclear and Quantum Engineering, KAIST

2014-2016 M.S., Department of Nuclear and Quantum Engineering, KAIST

학 회 활 동

Publication

1. Lee, Sang Hun, and Hyun Gook Kang. "Integrated societal risk assessment framework for nuclear power and renewable energy sources." Nuclear Engineering and Technology 47 (2015): 461-471.
2. Lee, Sang Hun, et al. "Reliability modeling of safety-critical network communication in a digitalized nuclear power plant." Reliability Engineering & System Safety 144 (2015): 285-295.

Proceedings

1. Lee, Sang Hun, and Hyun Gook Kang. "Preliminary Assessment of Population Dose during Nuclear Power Plant Normal Operation." IYNC 2014, Burgos, Spain, July 6-12, 2014.
2. Lee, Sang Hun, and Hyun Gook Kang. "Comparative Health Risk Assessment of CdTe Solar PV System and Nuclear Power Plant." ISOFIG/ISSNP 2014, Jeju, Korea, August 24-28, 2014.
3. Sung Min Shin, Sang Hun Lee, Han Seong Son, Seung Jun Lee and Hyun Gook Kang. "Test Based Reliability Quantification Method for a Safety Critical Software using Finite Test Sets." NPIC/HMIT 2015, Charlotte, N.C., February 23-26, 2015.
4. Lee, Sang Hun, and Hyun Gook Kang. "Measuring Risk Aversion for Nuclear Power Plant Accident: Results of Contingent Valuation Survey in Korea." Transactions of the Korean Nuclear Society Spring Meeting, Jeju, Korea, May 7-8, 2015.
5. Lee, Sang Hun, and Hyun Gook Kang. "Fault-Tree Modeling of Safety-Critical Network Communication in a Digitalized Nuclear Power Plant." Transactions of the Korean Nuclear Society Autumn Meeting, Gyeongju, Korea, October 29-30, 2015.
6. Lee, Sang Hun, and Hyun Gook Kang. "Reliability Assessment of Safety-critical Network Communication in Digitalized Nuclear Power Plant." 1st Asia-Pacific Young Practitioners'PRA (APYP-PRA) Forum, Heifei, China, November 3-4, 2015.