Annals of Nuclear Energy 108 (2017) 394–405

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Risk assessment of safety data link and network communication in digital safety feature control system of nuclear power plant

Sang Hun Lee [a], Kwang Seop Son [b], Wondea Jung [c], Hyun Gook Kang [a,*]

[a] Department of Mechanical, Aerospace, and Nuclear Engineering, Rensselaer Polytechnic Institute, Troy, NY, USA
[b] I&C/Human Factors Research Division, Korea Atomic Energy Research Institute, Daejeon, Republic of Korea
[c] Integrated Safety Assessment Division, Korea Atomic Energy Research Institute, Daejeon, Republic of Korea

ARTICLE INFO

Article history:
Received 30 December 2016
Received in revised form 13 April 2017
Accepted 17 April 2017
Available online 15 May 2017

Keywords:
Nuclear power plant
Digital I&C system
Safety data link
Safety data network
Probabilistic risk assessment

ABSTRACT

As one of the safety-critical systems in nuclear power plants (NPPs), the Engineered Safety Feature-Component Control System (ESF-CCS) employs safety data link and network communication for the transmission of safety component actuation signals from the group controllers to loop controllers to effectively accommodate various safety-critical field controllers. Since data communication failure risk in the ESF-CCS has yet to be fully quantified, the ESF-CCS employing data communication systems have not been applied in NPPs. This study therefore developed a fault tree model to assess the data link and data network failure-induced unavailability of a system function used to generate an automated control signal for accident mitigation equipment. The current aim is to provide risk information regarding data communication failure in a digital safety feature control system in consideration of interconnection between controllers and the fault-tolerant algorithm implemented in the target system. Based on the developed fault tree model, case studies were performed to quantitatively assess the unavailability of ESF-CCS signal generation due to data link and network failure and its risk effect on safety signal generation failure. This study is expected to provide insight into the risk assessment of safety-critical data communication in a digitalized NPP instrumentation and control system.

1. Introduction

Instrumentation and control (I&C) systems in nuclear power plants (NPPs) have recently been replaced with digital-based systems. As these systems generate a significant volume of data, interconnections between programmable logic controllers (PLCs) based on data communication protocol, which allow effective data transmission between PLCs for multiple operational functions including safety functions, have been employed to supplant conventional hard-wired signal transmission. The communication standards used for such PLCs in NPP digital I&C systems aim to provide flexibility in connecting different devices to each other without relying on fully-connected topologies, unlike commercial systems (Aldemir et al., 2007). For safety-critical applications, the commercial protocols have been altered to reach the high level of reliability required for safety system applications, and to eliminate the potential for uncertain timing to achieve deterministic safety criteria.

However, the primary issue of data communication in a digitalized safety-critical I&C system involves potential hazards, or a failure to communicate any necessary data when it is needed (Kisner et al., 2007). In terms of the data communication used for safety-critical information transmission in the NPP digital safety feature control system, the data link or data network failure will result in the loss of safety feature control via the control system, leading to mitigation action failure for a design basis accident (DBA). Therefore, the probability that safety-critical signal generation by an NPP digital I&C system becomes unavailable due to data communication failure must be quantitatively evaluated to address the communication risk into the system unavailability and the plant risk.

Previous studies conducted on the risk assessment of safety-critical communication in NPP digital I&C systems concerned a deterministic reliability assessment of a token ring protocol, which is a widely used protocol for controlled channel access in NPPs (Hong and Kim, 1997; Willig and Wolisz, 2001). They addressed reliability aspects related to protocol performance and the ring stability of the protocol in the presence of transmission error during Profibus operation based on a discrete time Markov chain.

Relatively few studies though have been performed to assess communication failure risk and to analyze its risk effects on the NPP safety-critical systems. In one such previous study, data trans-

* Corresponding author.
E-mail address: kangh6@rpi.edu (H.G. Kang).

http://dx.doi.org/10.1016/j.anucene.2017.04.025
0306-4549/

mission failure caused by network protocol failure in an NPP safety-critical I&C system was assumed to result in the total loss of safety component actuation control via the protection system (Kang and Jang, 2008). A limitation in the treatment of network communication protocol failure in this approach however is that the network protocol failure was treated as a catastrophic common cause failure (CCF) of communication modules in a digital I&C system. Since the safety functions of the protection system are allocated in redundant network channels and multiple field components are allocated to different PLCs to assure protection system diversity, the reliability model of data communication in NPPs must be constructed considering the protection system architecture along with the failure modes and causes of data communication failure. Other studies include modeling and analysis of controllers, software systems, and communication networks using a Petri net and dynamic flowgraph methodology (Jian and Shaoping, 2006; Al-Dabbagh and Lu, 2010). The limitations though of such dynamic modeling methods for data communication include the difficulty in integrating the model into a conventional plant probabilistic risk assessment (PRA) model which incorporates inter-system dependencies and human errors related to digital systems, as well as the digital equipment failures and their CCFs (Aldemir et al., 2006; Chu et al., 2008).

Subsequently, a proper PRA framework for assessing the reliability of a safety communication system should be developed by considering such characteristics as protocol and architecture in the safety-critical system. In previous authors' research, the hazard states and failure paths of Profibus protocol used for the data communication in the Engineered Safety Feature-Component Control System (ESF-CCS), which might lead a system to an unsafe state, are identified and the effect of important risk factors, such as periodic inspection period of communication modules, on engineered safety feature actuation signal (ESFAS) generation unavailability was quantified (Lee et al., 2015).

The current work is an extension of this prior study and aims to address issues regarding the risk assessment of both data link and data network communication, namely ESF-CCS signal generation failure in consideration of the various types of ESF-CCS interconnection layouts as well as the reliability of the fault-tolerant algorithm implemented for data network for utilizing a redundant bus structure. In order to assess the data communication risk and its effect on ESFAS generation failure and obtain risk information, a fault tree model of signal generation failure in an engineered safety feature (ESF) component that considers communication failure between group controllers (GCs) and loop controllers (LCs) in the ESF-CCS is developed and integrated into a plant risk model.

2. Target system

2.1. Engineered Safety Feature-Component Control System

The Advanced Power Reactor 1400 (APR-1400) man-machine interface system (MMIS) architecture was developed based on digital safety-critical systems, with the ESF-CCS developed to meet the design requirements of the APR-1400 as shown in Fig. 1 (Lee et al., 2008). The functions of the digital engineered safety feature actuation system and field actuator controllers in the preceding Optimized Power Reactor 1000 (OPR-1000) are expected to be performed by the ESF-CCS; that is, the ESF-CCS provides an initiation signal to each independent ESF component that require automatic actuation when abnormal conditions are detected. In order to effectively accommodate the huge number of field controllers in the ESF-CCS, two types of data communication systems, the High Reliability-Safety Data Link (HR-SDL) and High Reliability-Safety Data Network (HR-SDN), were employed for the transmission of safety-critical information from GCs to LCs. The following sections provide a detailed description of each system and the interconnections between the GCs and LCs in the ESF-CCS.

2.2. High Reliability-Safety Data Link communication

The HR-SDL communication system uses the Profibus-Fieldbus Data Link (Profibus-FDL) based on send data with no acknowledge (SDN) (Kim et al., 2007). HR-SDL is a safety-graded communication module for transmitting safety-critical signals, and it uses deterministic protocol to secure real-time operation and unidirectional peer-to-peer communication methods to only allow communication through a dedicated link between two communication modules, where fiber-optic cable is used as a physical link for physical isolation.

In the ESF-CCS, a single GC must be connected to twelve LCs with separate physical links for physical isolation while the HR-SDL supports two peer-to-peer communication ports; therefore, an optical splitter module (NFD1S-1Q) is used for 1-to-N communication between the GCs and LCs (Lee et al., 2013). It is notable that there are two types of HR-SDL modules: fiber optic transceivers (NFD1-6Q) and RS-485 transceivers (NFD1-5Q), which use optical and electrical signals, respectively. The NFD1S-1Q converts the electrical signal received from the NFD1-5Q module in the GC by RS-485 to four identical optical signals, which are separately transmitted to each NFD1-6Q module in the LC located in the same division. A simplified configuration of HR-SDL connections between a GC and four LCs in the same ESF-CCS channel is shown in Fig. 2.

2.3. High Reliability-Safety Data Network communication

While the HR-SDN communication system also uses Profibus-FDL protocol based on SDN communication like the HR-SDL, physically the HR-SDN follows a bus topology. Based on the shared network bus medium, HR-SDN communication module provides N-to-N safety-critical data exchange which allows deterministic data exchange and broadcasting through network buses between safety-graded PLCs in a multi-drop fashion (Lee et al., 2008).

Compared to the HR-SDL system which is composed of peer-to-peer connection between communication modules, redundant network modules and buses are implemented in the HR-SDN system for diversity in order to ensure reliable ESF actuation signal transmission in the ESF-CCS, as shown in Fig. 3 (Lim et al., 2006). In each division, there are doubly redundant network channels, e.g. Primary NET and Standby NET, which are connected to the HR-SDN modules in each controller and transmit a data frame from GCs to LCs. Each LC consists of a main LC and a hot-standby backup LC where each controller performs the function of two-out-of-three component control auctioneering of the signals received from the three GCs in the same division.

One of the important features of the digital I&C systems in NPPs is fault-tolerance. For NPP communication systems having redundant network channels, various fault-tolerant schemes have been employed to increase the reliability of data transmission. In general, these schemes include fault detection through the use of isolation equipment or protocols that limit the extent and propagation of a fault, and fault removal by automatically reconfiguring transmission paths around failed links (Kisner et al., 2007).

For the HR-SDN system having redundant network channels, both fault-detection and fault-removal algorithms are implemented on the receiver side of the network modules; in other words, the hot-standby backup LC takes over the task when a malfunction of the main LC is detected in order to ensure ESF actuation signal transmission between GCs and LCs (Lim et al., 2006). The algorithm checks whether all data is received by the network mod-

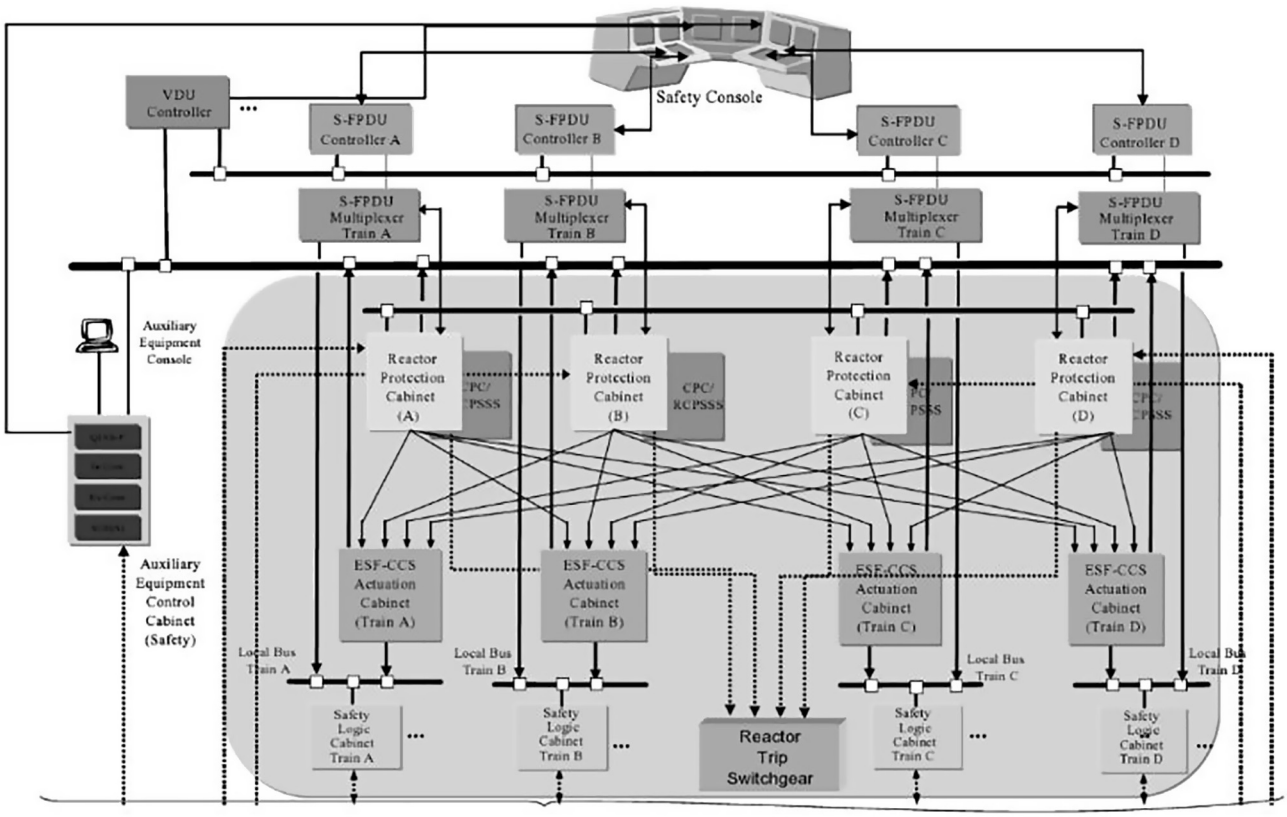


Fig. 1. APR-1400 MMIS architecture.

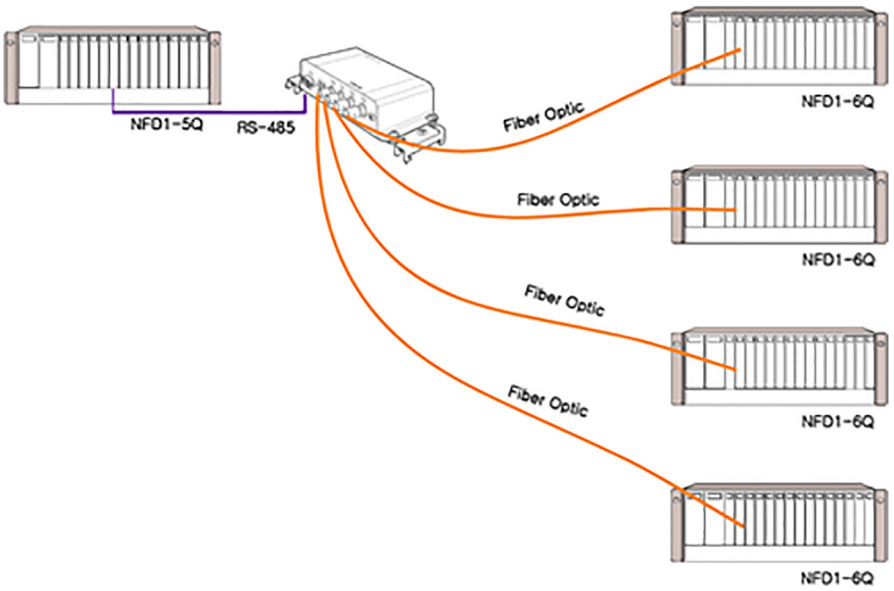


Fig. 2. Interconnection between HR-SDL communication modules in the ESF-CCS.

ule and the checksum is then recalculated and compared with the original one attached to the transmitted data to check for checksum error. If any of the data is missing or the checksum is corrupted, a network error is detected and the operational network channel is switched to an intact network channel. It is notable that this process is accomplished by a separate software function dedicated to the fault-tolerant algorithm in the HR-SDN module. The summarized logic of the fault-tolerant mechanism implemented in an HR-SDN communication module utilizing redundant network buses for reliable data transmission in the ESF-CCS is shown in Fig. 4.

3. Model development

Since the function of the ESF-CCS is to initiate emergency actuations to mitigate the DBAs of a NPP, the top event of data commu-

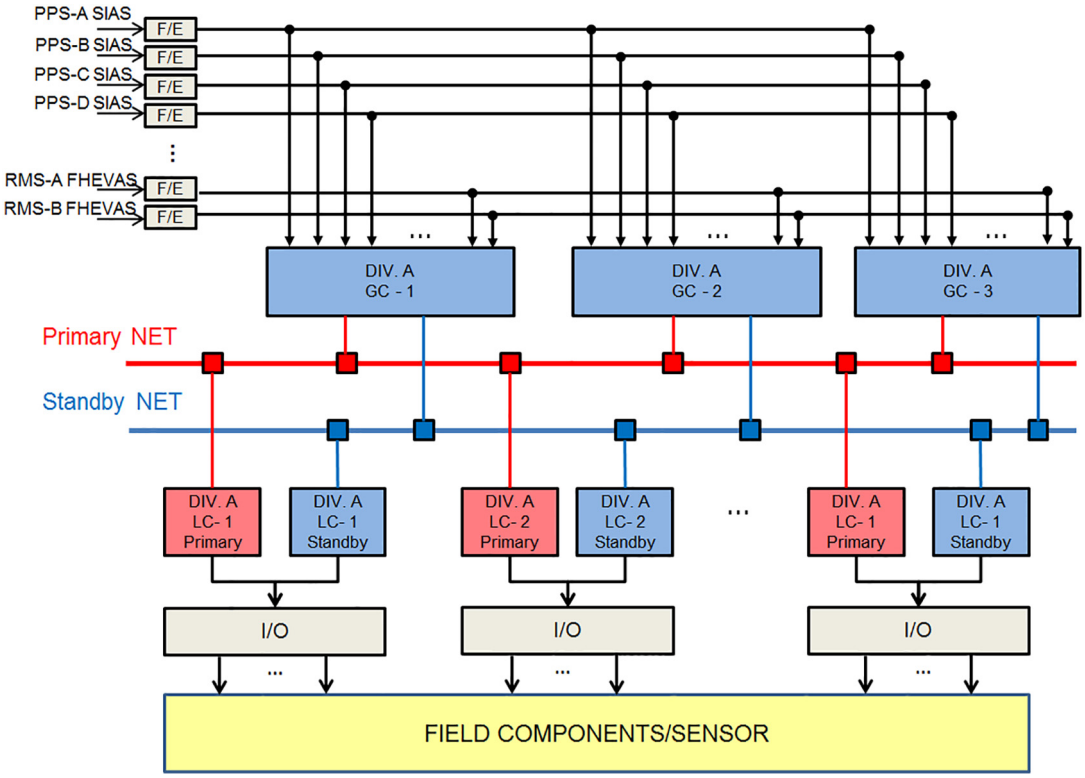


Fig. 3. Configuration of the ESF-CCS applied with HR-SDN communication system.

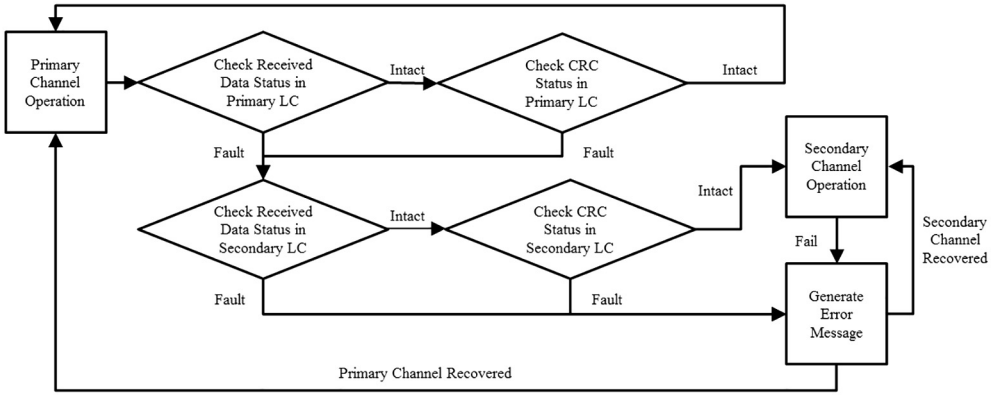


Fig. 4. Logic of the network fault-tolerant algorithm implemented in HR-SDN.

nication failure is the ESFAS generation failure for the ESF components via ESF-CCS. The fault trees for HR-SDL and HR-SDN data communication failure were developed considering the hazardous states due to data communication failure that can lead to the top event, and the logical interrelationships of failure mechanisms that can lead to the failure of safety-critical data transmission, based on authors' previous research (Lee et al., 2015). The fault tree is then tailored to its top event which corresponds to a particular ESFAS generation failure and integrated into a plant PRA model to address the risk effect of data link and data network failure on ESF-CCS signal generation failure. In this study, the functional failure of each communication module in the PLCs is modeled as a basic event in the fault tree. The failure of communication module can be caused by the failure of both hardware components and dedicated software functions in the module, and the token or data frame corruption caused by noise in the transmission medium.

3.1. Modeling of programmable logic controller modules

ESF-CCS design is based on a PLC, which consists of various modules such as processor, digital input/output, and communication modules. For the controllers in the ESF-CCS, digital input modules in the GCs interface with the ESF initiation signals from the plant protection system (PPS). The processor module in the GC performs auctioneering through four channel inputs from the PPS. If a specific ESF signal is generated based on the auctioneering results, the GCs provide safety-critical information to the LCs in the same division, and then digital output modules in the LCs transfer the actuated automatic control signals to the field components. Here, the communication module, which includes a processor unit and a driver unit to execute the software functions for Profibus protocol, is used for performing field bus communication between GCs and LCs in the ESF-CCS.

In case of the HR-SDL, the communication module consists of two boards: the communication processor board (CPB) and the driver board (DRB). These boards are connected by a piggy back connector to each other, as shown in Fig. 5 (Choi et al., 2008). The CPB provides an interface between the processor module (PM) and the DRB, while the DRB is interfaced with the CPB and other PLCs through two communication ports. On the other hand, the HR-SDN module (NFD2-2Q) consists of a single board including two separate CPUs for communication processing (XC161) and a driver (DSTnI-LX) with dedicated software functions, as shown in Fig. 6 (Park et al., 2008). The driver board responsible for data exchange between other PLCs supports a single communication port connected to a shared bus medium in a multi-drop fashion. Both communication modules perform the same safety software functions for data transmission between GCs and LCs in the ESF-CCS, which are graded as safety-critical software, as shown in Table 1 (Lee et al., 2008).

3.2. Quantification of basic event probability

The functions of the HR-SDL and HR-SDN systems are performed by hardware components and software in the communication modules of the GCs and LCs in the ESF-CCS. Failure of either hardware module or the dedicated software function may cause data communication failure, resulting in a failure to generate the ESF actuation signal in an ESFAS condition. In addition, token or data frame corruption caused by bit errors due to the introduction of noise in the transmission medium can also cause an incorrect frame to be received by the module, thus resulting in a failure of ESFAS generation. To assess the unavailability of ESF-CCS signal generation due to data link and data network failure and its risk effect on ESF-CCS signal failure in an ESF initiation condition, a quantification scheme for each failure cause and the assumptions used in the model are summarized as follows.

For the newly developed digital PLC modules, failure probability data from design documents is used as shown in Table 2 (Choi, 2007; Hur et al., 2013). It was assumed that the components are tested at least once per month and the repair time of the PLC modules, when a fault was detected by the self-diagnostic function, was assumed as eight hours. The unavailability of the optical splitter module was estimated based on the base failure rate of a fiber optic splitter (Berghmans et al., 2008). In this study, the fail-to-hazard probability of the intersystem data bus and the back plane of the PLCs were ignored since it was assumed that their failure can be treated in a safe manner.

In terms of software failure, as the software takes inputs from other systems and produces outputs that are used either by operators or by other software and hardware, it can be treated with a probability method. In this study, since the communication software in the ESF-CCS GCs and LCs is graded as safety-critical software based on its design specification, as shown in Table 1, the software integrity level (SIL) of the network module software is assumed as SIL-4, and the software failure probability as 1.0E−05 according to the SIL-4 target of IEC 61508 (Brown, 2000) based on Table 3.

It is expected that the PLC module redundancies in the ESF-CCS make the probabilities of the CCFs dominant. In particular, to model the failure of multiple identical communication modules in the GCs and LCs in the same division of the ESF-CCS as a result of shared causes, the CCF of the communication modules in each LC and GC must be considered as each LC and GC uses the same communication module and implemented software function, respectively. In the present work, in order to analyze the CCF regarding data communication failure in the ESF-CCS, the CCFs of hardware are considered assuming the beta factor to be one-tenth, based on the beta factor model (Authen and Holmberg, 2012). In case of software failure, since the installation of the same software in redundant channels or systems may remove the redundancy effect, the communication software failure is conservatively assumed to induce the CCF of each GC and LC communication modules in the ESF-CCS.

Since the Profibus protocol employs coaxial cables or broadband as a transmission medium, 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. While safety-critical instrumentation generally falls into one of two operation modes which is continuous and low demand mode (Brown, 2000), the NPP safety-critical I&C system is operated as low demand mode since its safety function is called up on at the time point of demand when NPP is at abnormal state. Therefore, the probability of error introduction in the transmitted safety-critical data frame via network communication in the ESF-CCS in ESF actuation condition, which may result in hazardous states, can be treated as the probability of failure on demand.

In this study, bit error rate (BER) is used to assess ESF-CCS signal generation failure probability due to medium-related bit error. BER is defined as the ratio of the number of bits received incorrectly to the total number of bits transmitted per unit time, as shown in Eq. (1). Based on Eq. (1), the expected number of erroneous bits in the

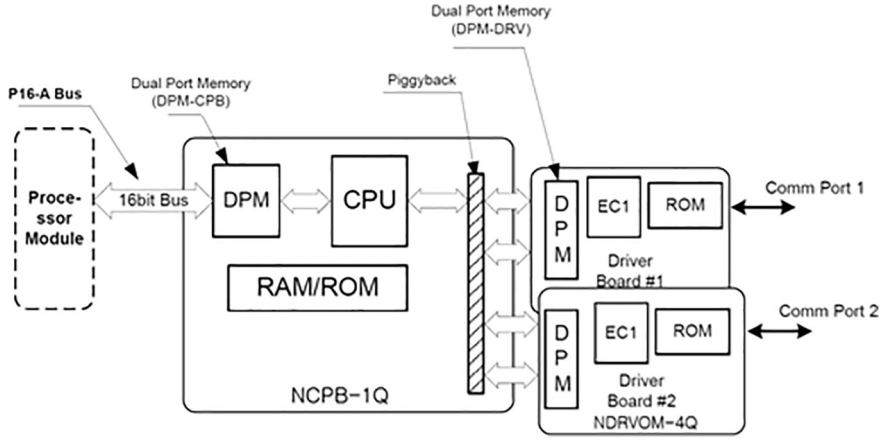


Fig. 5. Hardware structure of HR-SDL communication module.

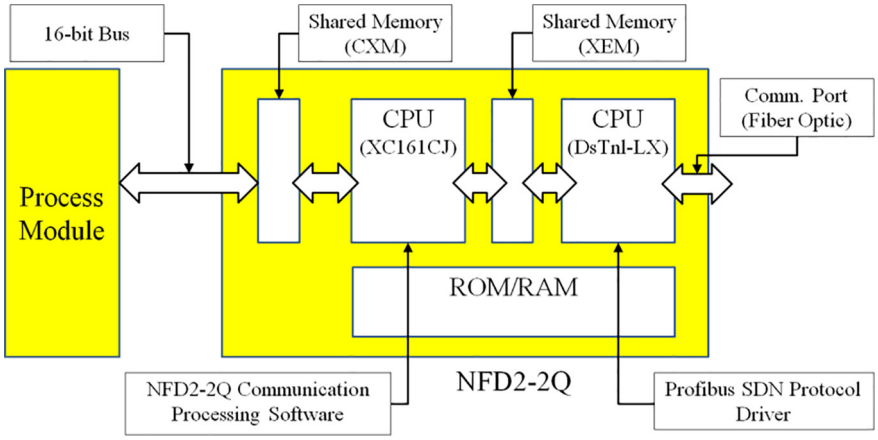


Fig. 6. Hardware structure of HR-SDN communication module.

Table 1
Software specification of safety-critical communication modules in ESF-CCS.

Software	Major software functions	Safety grade
Communication Processor (CP) Software	- Data exchange between CP and processor - Data exchange between CP and DR - Error management for CP and DR	Safety-critical (SC)
Communication Driver (DR) Software	- Data exchange between CP and other stations - Error management for DR	Safety-critical (SC)

Table 2
Unavailability of PLC modules in ESF-CCS.

Module	Unavailability
Processor module	3.03E−04
Analog input module	3.53E−04
Digital input module	3.53E−04
Digital output module	7.92E−05
HR-SDL CPB module (NCPB-1Q)	2.29E−05
HR-SDL DRB module (NDRVOM-4Q)	3.96E−05
Optical splitter module (NFD1S-1Q)	6.57E−05
HR-SDN module (NFD2-2Q)	9.78E−05

Table 3
Software integrity levels and corresponding reliability targets from IEC 61508.

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

transmitted token or data frame between GCs and LCs in the ESF-CCS is estimated and treated as the probability of each frame corruption caused by bit errors in the bus medium, considering the length of transmitted frames between controllers, as shown in Fig. 7 (Lee et al., 2008), and assuming the BER equal to that of a general Profibus physical layer which is on the order of 1.0E−08 (Irwin, 1997).

$$\text{BER} = \frac{\text{Expected number of erroneous bits}}{\text{Total number of transmitted bits}} \quad (1)$$

As mentioned above, a fault-tolerant algorithm is implemented in the HR-SDN communication module for utilizing redundant channels to help network communication system correctly perform its intended functions in spite of the presence of network faults. In the evaluation of fault-tolerance of such system, the failure detection coverage, which is a measure of the system's ability to perform failure detection, failure isolation, and failure recovery, is a crucial factor (Dugan and Kishor, 1989; Lee et al., 2006, 2014). Based on the study of Lee et al. (2006), the fault detection coverage of the checksum for CPU errors in the NPP digital plant protection system can be assumed to be approximately 0.7. Since the ESF-CCS is a newly developed system, the detailed fault coverage or reliability of the fault-tolerant algorithms implemented for the HR-SDN network system was yet evaluated. In this study, the failure probability of the fault detection algorithm by checksum and the removal algorithm for reconfiguring the HR-SDN network path when a network fault is detected were conservatively assumed to be 0.7 as a base case. In addition, in order to analyze the effect of fault coverage on ESF-CCS signal generation unavailability, the coverage of the fault-tolerant algorithms for the HR-SDN system having redundant network channels was assumed to be in the range of 0.7 to 0.99 as a sensitivity study.

Apart from the automatic ESF actuation signal generation by the ESF-CCS, diverse manual actuation (DMA) switches provide a redundant means for the operator in the main control room to access the field components via hard-wired path, thereby allowing a human operator to manually actuate the ESF components as a backup of an automated system via ESF-CCS. However, it is difficult to estimate the human operator failure probability since the main control room of the APR-1400 is still under design, and manual actuation largely depends on the accident situation, the operating environment, and provided information. In this study, human operator action failure is modeled in the fault tree and the failure probability of the human operator for manual actuation of ESF actuation via DMA was assumed as 0.1, based on the conventional human error probability method (Kang et al., 2009).

3.3. Fault tree model development for system unavailability and network risk effect analysis

The top event of the system unavailability model in this study is the failure of corresponding ESFAS generation for each ESF component. The fault tree model of GC-LC communication failure is constructed based on the RM-ESFCCS, which was originally established by previous study (Kang and Jang, 2008) and further developed by considering the detailed layout of each network sys-

Header	Start Delimiter (SD)	Destination Address (DA)	Source Address (SA)	End Delimiter (ED)
Length	1 byte	1 byte	1 byte	1 byte

(a)

Header	Start Delimiter (SD)	Destination Address (DA)	Source Address (SA)	Frame Control (FC)	Data Unit (DU)	Frame Check Sequence (FCS)	End Delimiter (ED)
Length	1 byte	1 byte	1 byte	1 byte	8 bytes	1 byte	1 byte

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 signal of GC	INTEGER	1	3000 ~ 3255 4000 ~ 4255 5000 ~ 5255

(b)

Fig. 7. Description of Profibus protocol frame structure for (a) token frame format, and (b) data frame format with fixed length of data units transmitted from GC to LC.

tem as well as the hazard states and failure paths of data communication systems between GCs and LCs. While the traditional single-controller system utilizes dedicated processors for each component, the ESF-CCS provides an initiation signal to various independent ESF functions and ESFAS-required safety components used for DBA mitigation measures in NPPs are functionally allocated in the LCs of each division of the ESF-CCS, as shown in Table 4.

The current work develops a fault tree model for ESF-CCS signal failure for the sump isolation valve SI-V675 as a case study. The sump isolation valve initiated by recirculation actuation signal (RAS) is used for reactor coolant recirculation in both long-term core cooling and containment cooling management, and is considered to be one of the important ESF components in terms of plant risk. It should be noted that as the ESF-CCS is still in the design phase and the modules are still being improved, the models developed in this study represent an interim design alternative.

3.3.1. Development of a fault tree model for HR-SDL network communication

The logic of the developed model describing ESFAS generation failure for sump isolation valve SI-V675 initiated in RAS within the ESF-CCS system applied with HR-SDL communication (comprising of data link based on peer-to-peer connection between communication modules) is shown in Fig. 8. In terms of the signal failure for a field component due to LC signal processing, both independent failure and the CCF of the digital input/output and processor modules in the LC may cause a failure of LC signal processing. In addition, ESFAS failure can be caused by the failure to provide input signals to the LC including data transmission failure between GCs and LC A4, and the failure of LC input signal generation by the GCs in the same division.

Fig. 9 shows the developed fault tree model of safety signal input reception by LC. Since the LC receives the data frame for ESF component actuation, transmitted from the GCs in the same division, a failure of data communication between GCs and LCs in the same division includes the failure of both hardware and on-demand software failure of HR-SDL module as well as the failure due to transmission-medium-related bit errors in the received data frames from the three GCs in the same division.

The failure to provide input to the LCs can also be caused by the failure of input processing by GCs. Since the LC processes the transmitted GC signals via communication module based on two-out-of-three voting logic, LC failure of input processing can be caused by independent failure and the CCF of the digital input/output and processor modules in the GC. In addition, the failure of the optical splitter module used for 1-to-N communication between GCs and LCs in the HR-SDL system is modeled for each GC. Fig. 10 shows the developed fault tree model for the failure of LC safety signal input generation and transmission by GC.

Table 4
Example of LC allocation to ESF components in ESF-CCS.

ESFAS	Required ESF component actuation	Description	LC allocation
RAS-A	V675 HX1A	CIV SI-V675 Spray Hx. A inlet isol. v/v CC-V141	LC A4 LC C4
RAS-B	V676 HX1B	CIV SI-V676 Spray Hx. A inlet isol. v/v CC-V142	LC B4 LC D4

3.3.2. Development of a fault tree model for HR-SDN network communication

Fig. 11 presents the logic of the developed model for ESFAS generation failure of SI-V675 in RAS for the ESF-CCS system applied with HR-SDN comprising a redundant network. Compared to the HR-SDL network, signal failure due to LC signal processing includes not only independent failure and the CCF of the digital input/output and processor modules in LC but also the failure of the heartbeat algorithm, which is responsible for allowing the standby LC processor module to generate an ESF component actuation signal when the main LC processor module fails to function. In addition, ESFAS generation failure can be caused by a failure to provide input to the both the main LC (LC A4-A) and the hot-standby backup LC (LC A4-B) in the redundant network channel.

Considering that both HR-SDL and HR-SDN communication modules conduct the same function in the ESF-CCS, which is LC input signal transmission from the GC for ESFAS generation, the

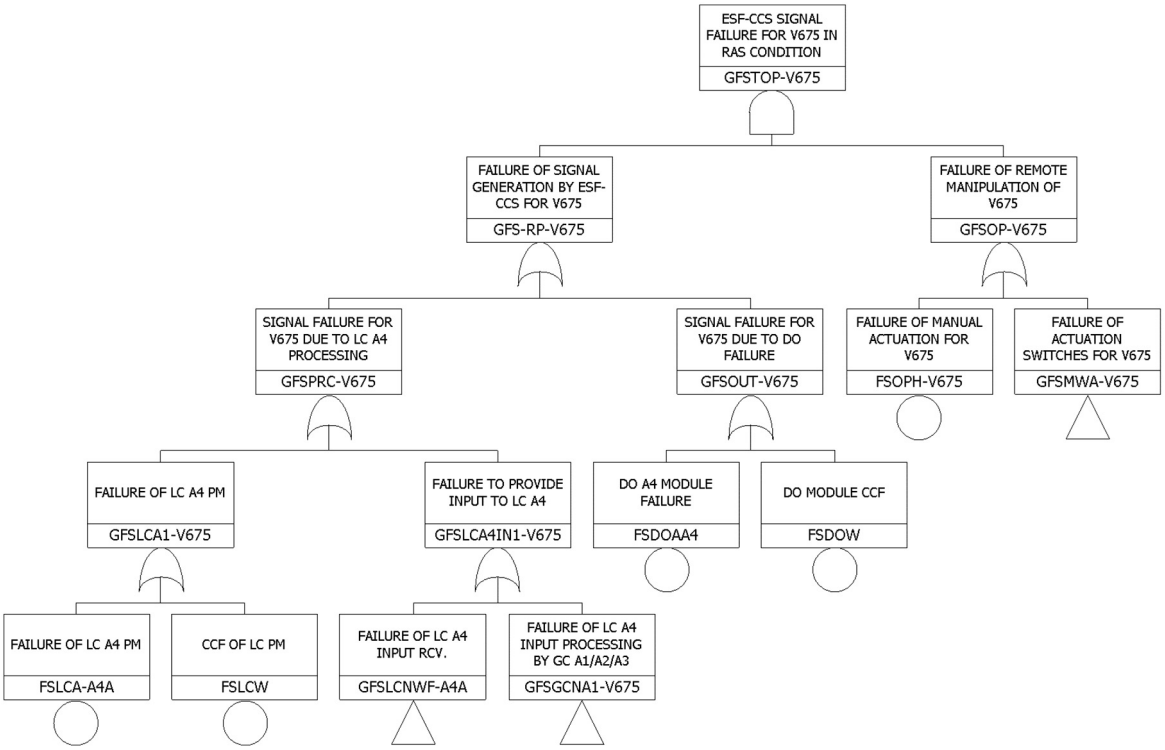


Fig. 8. Top logic of the developed fault tree model of ESF-CCS with HR-SDL.

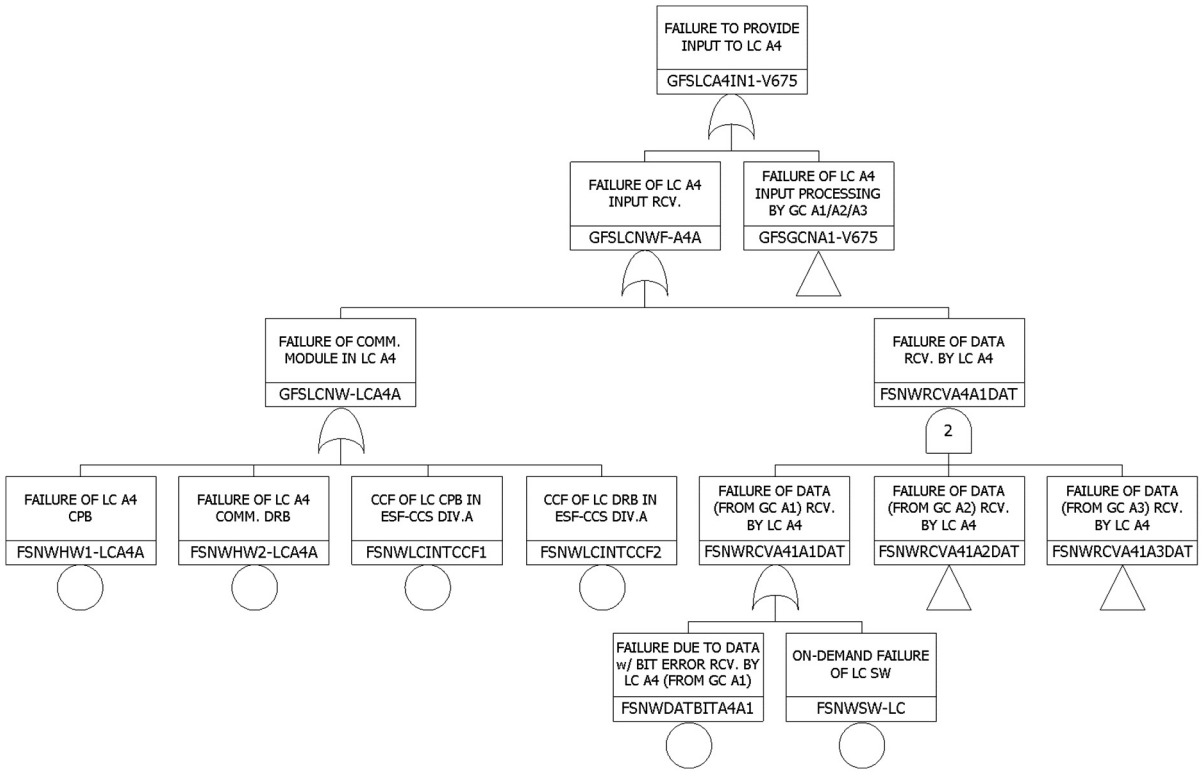


Fig. 9. Logic of the failure of LC A4 input reception for SI-V675 actuation.

developed logic for HR-SDN communication failure can be modeled in a similar manner as the HR-SDL communication model. That is, the network failure in each LC includes both the failure of the HR-SDN module and the communication protocol. Compared to HR-SDL case, a redundant network bus structure is implemented in the HR-SDN network system, so the failure of network communication between the GCs and LCs can be caused by the failure to provide input to both the main and hot-standby backup LCs.

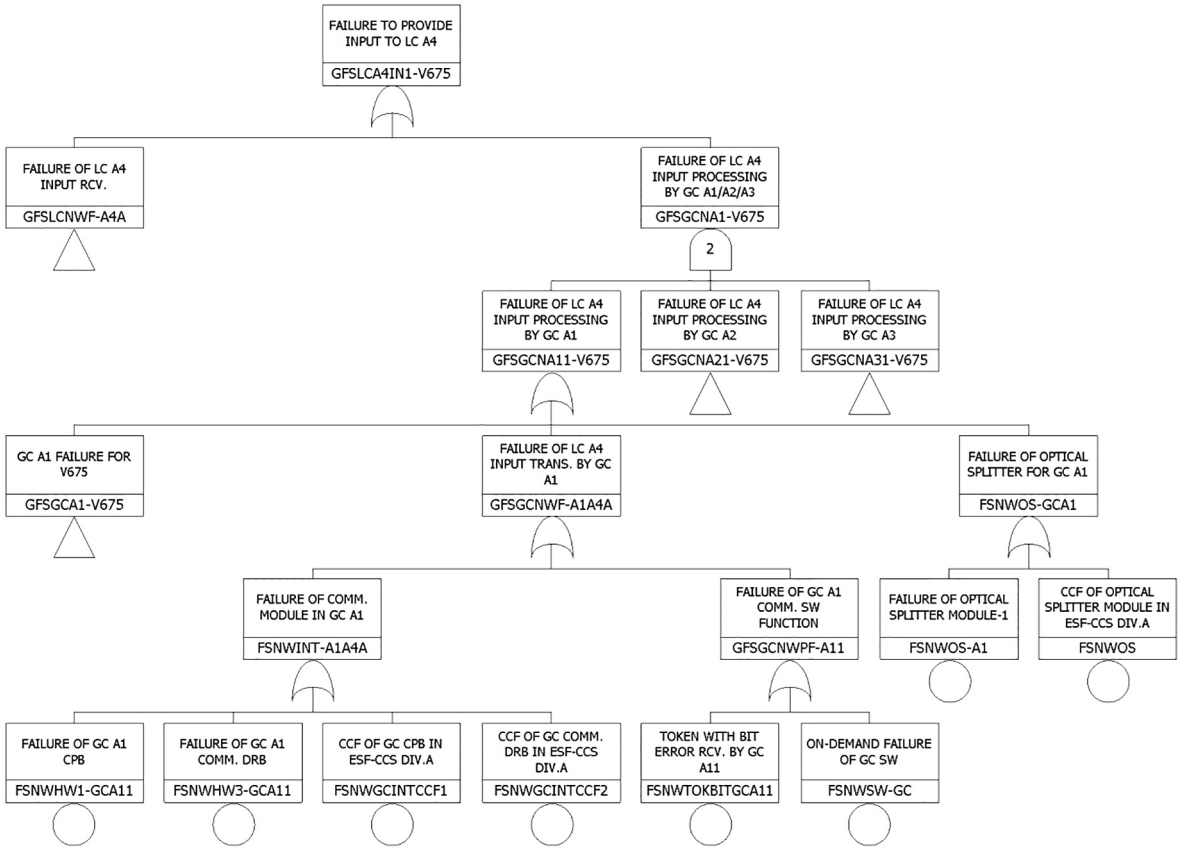


Fig. 10. Logic of the failure of LC A4 input processing by GC for SI-V675 actuation.

In addition, the fault-tolerant algorithm is implemented in the HR-SDN system for reliable data transmission to utilize the redundant channel when a network fault is detected in either channel. The combination of a failure of the fault-tolerant algorithm, which includes both fault detection and removal algorithms, with the failure of either network channel may cause a fault detection failure in the failed network channel, resulting in the failure to provide input to both LCs in ESFAS condition. Therefore, the failure of both network fault detection and removal algorithms are modeled as basic events in the developed fault tree model.

4. Results

Based on the developed fault tree models for the ESF-CCS applied with HR-SDL and HR-SDN systems, the unavailability of ESF-CCS signal generation due to data link or network failure and their risk effect on safety signal generation failure was estimated. In each case, the top event cutset was generated using the Advanced Information Management System for Probabilistic Safety Assessment (AIMS-PSA) (Han et al., 2008) and the unavailability of ESFAS generation was estimated based on a minimal cutset (MCS) analysis. In this study, the overall communication failure risk was calculated as the sum of the failure probabilities of the MCSs related to communication failure, namely the hardware failure, and the software failure of the communication module, and the failure due to token or data frame corruption caused by noise in the transmission medium. The risk effect of the data link or network failure on ESFAS unavailability was estimated as the sum of Fussell-Vesely (FV) importance of the MCSs related to the communication failure basic events.

4.1. Signal unavailability due to communication failure

The ESF-CCS utilizes data communication for safety-critical signal transmission, therefore the communication failure in the GCs or LCs in the same division causes a loss of input to the LCs; that is, the GCs cannot transmit a demand signal to the LCs with the failure of data communication, resulting in ESFAS generation failure via ESF-CCS. Based on varying design specifications for digitalized NPPs applied with the ESF-CCS (Kang and Jang, 2008; Lee et al., 2008), risk quantification was performed by analyzing the MCSs and the basic events related to network failure to address the risk issues regarding three representative designs of the ESF-CCS applied with data communication, as follows:

- Case 1: HR-SDL system, characterized by data link communication based on peer-to-peer connection between GCs and LCs in the ESF-CCS.
- Case 2: HR-SDN system having a single network channel for data network communication between GCs and LCs in the ESF-CCS.
- Case 3: HR-SDN system having a redundant network channel with fault coverage of 0.7 for fault-tolerant algorithms implemented for data network communication between GCs and LCs in the ESF-CCS.

As a result, the dominant MCSs of cases 1 and 2 included the independent failure of the LC processor module, digital output module, the CCF of the refueling water tank (RWT) level sensors, and the failure of the LC communication module. Since no redundancy for the communication path in the ESF-CCS was assumed in cases 1 and 2, the failure of a LC communication module was

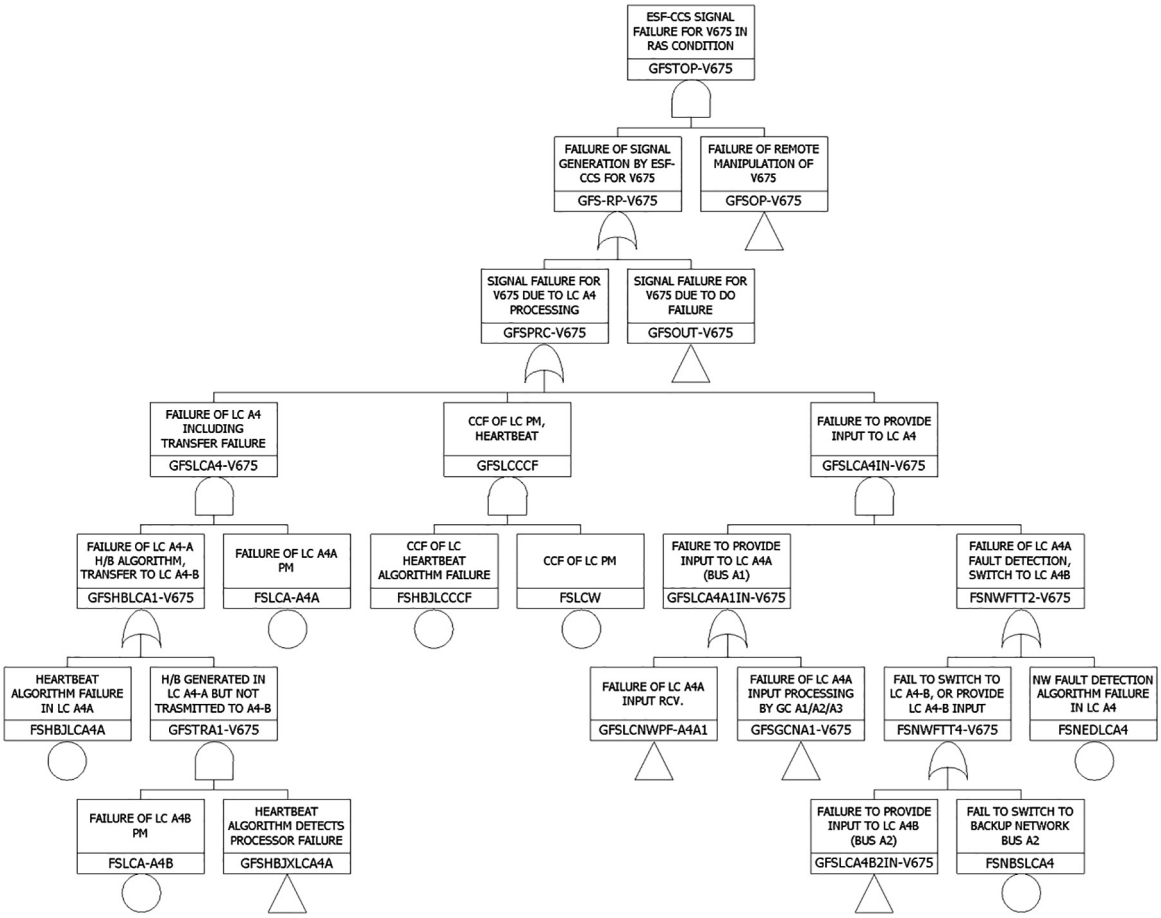


Fig. 11. Top logic of the developed fault tree model of ESF-CCS with HR-SDN.

considered as one of the dominant factors which cause the failure of ESF-CCS signal generation. On the other hand, the dominant MCSs of case 3 included both the failure of a single network channel combined with the failure of the fault-tolerant algorithms, and the CCF of PLC modules including communication modules and sensors, as shown in Fig. 12. This result implies that the dominant factor determining ESFAS unavailability related to communication failure in case 3 includes both the failure of the fault-tolerant algorithms for the HR-SDN system having a redundant network channel (FSNEDLCA4: Network fault detection algorithm failure in LC A4, FSNBSLCA4: Network fault recovery algorithm failure in LC A4), and the CCF of communication module failure.

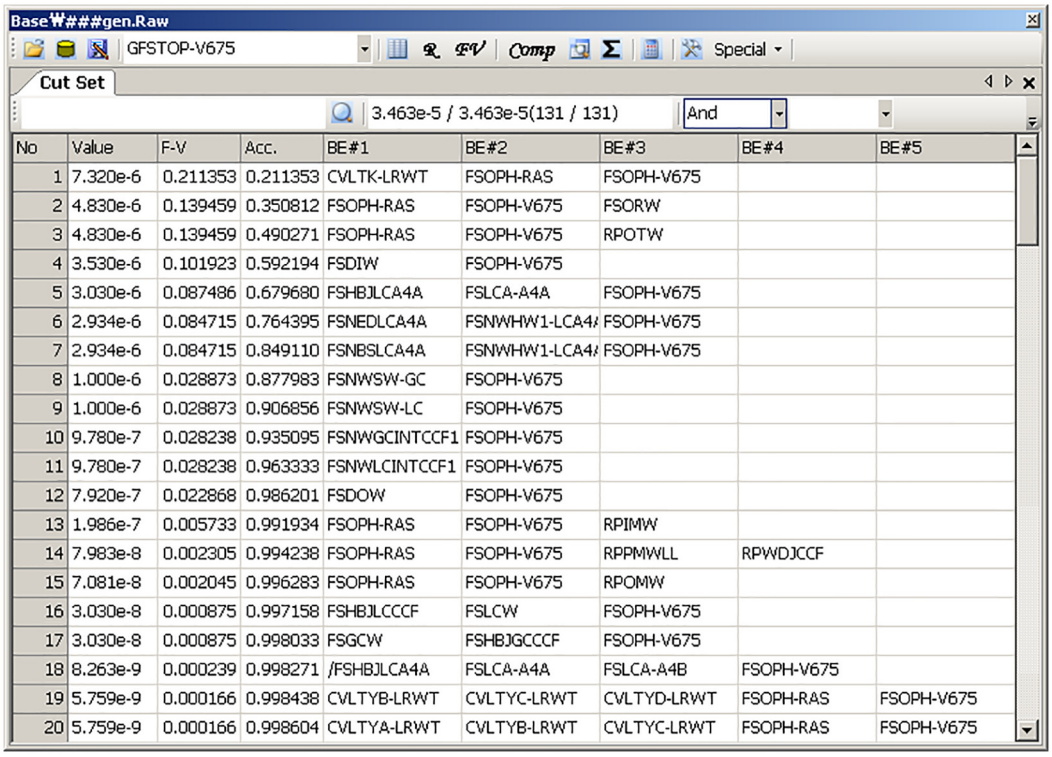
Based on the analyzed top-event MCSs, the unavailability of ESFAS generation for SI-V675 in RAS and related communication failure were quantified. Table 5 shows the summary of the quantification results for each case. It is demonstrated that the unavailability of ESFAS generation due to data communication failure in case 2 is higher than that in case 1 since the failure of the LC communication modules is the dominant MCS for communication failure, and the failure probability of HR-SDN module is higher than that of HR-SDL module. On the other hand, the unavailability of ESFAS generation due to data communication failure is lower in case 3 because the network channel redundancy reduces the effect of communication module failure in a single channel by a factor of the fault coverage of the fault-tolerant algorithms implemented in the HR-SDN module. This result implies that the fault coverage of the fault-tolerant algorithms is the important factor that determines ESFAS generation unavailability due to network failure for the HR-SDN system having a redundant network channel.

4.2. Risk effect of network failure on safety signal unavailability

As mentioned above, one of the important basic events for redundant HR-SDN system consists of the failure of the LC network module in a single network channel in combination with the failure of the fault-tolerant algorithms, as shown in the quantification result of case 3. That is, the failure of a single network channel with fault detection algorithm failure, or the failure of the fault removal algorithm to switch to the intact network channel when a fault is detected in the other channel, can both cause ESFAS generation failure via ESF-CCS. In this study, in order to analyze the effect of fault-tolerant algorithm failure on the reliability of the HR-SDN network system, sensitivity studies were conducted based on case 3 in Section 4.1 by ranging the fault coverage of such fault-tolerant algorithm from 0.7 to 0.99.

As shown in Fig. 13, the quantification results demonstrate that high fault coverage of the fault-tolerant algorithms effectively decreases the risk effect of network failure. Note that C_1 and C_2 denote the fault detection coverage and the fault recovery algorithm for network faults in the HR-SDN module, respectively. The risk effect of network failure on ESFAS generation unavailability decreases from 24.08% to 16.62% when the fault coverage of fault detection (C_1) increases from 0.7 to 0.99, assuming the coverage of fault recovery algorithm (C_2) as 0.9.

Compared to the conventional peer-to-peer data link method, i.e. HR-SDL system, where the risk effect of data communication failure on ESFAS generation unavailability was estimated as 13.90%, as shown in Table 5, the quantification results for both network protocols applied in the ESF-CCS revealed the potential appli-



No	Value	F-V	Acc.	BE#1	BE#2	BE#3	BE#4	BE#5
1	7.320e-6	0.211353	0.211353	CVLTK-LRWT	FSOPH-RAS	FSOPH-V675		
2	4.830e-6	0.139459	0.350812	FSOPH-RAS	FSOPH-V675	FSORW		
3	4.830e-6	0.139459	0.490271	FSOPH-RAS	FSOPH-V675	RPOTW		
4	3.530e-6	0.101923	0.592194	FSDIW	FSOPH-V675			
5	3.030e-6	0.087486	0.679680	FSHBJLCA4A	FSLCA-A4A	FSOPH-V675		
6	2.934e-6	0.084715	0.764395	FSNEDLCA4A	FSNWHW1-LCA4A	FSOPH-V675		
7	2.934e-6	0.084715	0.849110	FSNBSLCA4A	FSNWHW1-LCA4A	FSOPH-V675		
8	1.000e-6	0.028873	0.877983	FSNWSW-GC	FSOPH-V675			
9	1.000e-6	0.028873	0.906856	FSNWSW-LC	FSOPH-V675			
10	9.780e-7	0.028238	0.935095	FSNWGCINTCCF1	FSOPH-V675			
11	9.780e-7	0.028238	0.963333	FSNWLCINTCCF1	FSOPH-V675			
12	7.920e-7	0.022868	0.986201	FSDOW	FSOPH-V675			
13	1.986e-7	0.005733	0.991934	FSOPH-RAS	FSOPH-V675	RPIMW		
14	7.983e-8	0.002305	0.994238	FSOPH-RAS	FSOPH-V675	RPPMWLL	RPWDJCCF	
15	7.081e-8	0.002045	0.996283	FSOPH-RAS	FSOPH-V675	RPOMW		
16	3.030e-8	0.000875	0.997158	FSHBJLCCCF	FSLCW	FSOPH-V675		
17	3.030e-8	0.000875	0.998033	FSGCW	FSHBJGCCCF	FSOPH-V675		
18	8.263e-9	0.000239	0.998271	/FSHBJLCA4A	FSLCA-A4A	FSLCA-A4B	FSOPH-V675	
19	5.759e-9	0.000166	0.998438	CVLTYB-LRWT	CVLTYC-LRWT	CVLTYD-LRWT	FSOPH-RAS	FSOPH-V675
20	5.759e-9	0.000166	0.998604	CVLTYA-LRWT	CVLTYB-LRWT	CVLTYC-LRWT	FSOPH-RAS	FSOPH-V675

Fig. 12. Dominant minimal cutsets of the case 3 fault tree (RAS signal failure by LC A4-A and -B for field component SI-V675 for HR-SDN having redundant network channels).

Table 5
Quantification results of ESFAS unavailability considering network risk in the case studies.

	Case 1	Case 2	Case 3
Network system	HR-SDL	HR-SDN	HR-SDN
Channel redundancy	X	X	O
ESF-CCS signal failure for SI-V675 in RAS condition	7.32e−05	7.67e−05	3.46e−05
Unavailability of ESFAS generation due to network failure	1.02e−05	1.37e−05	9.82e−06

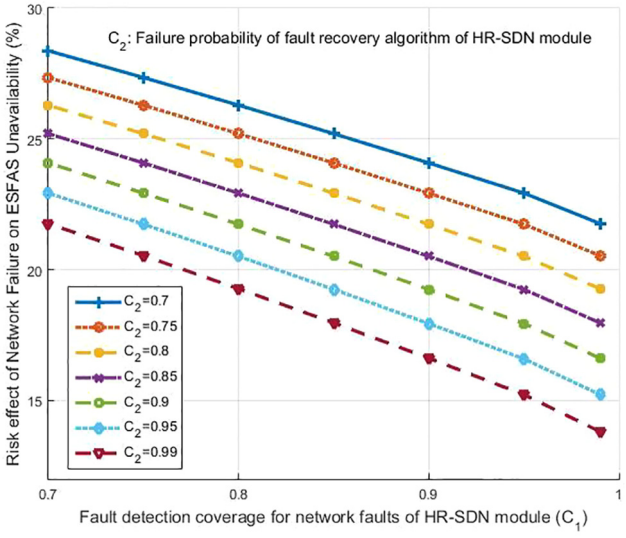


Fig. 13. Risk effects of network failure on ESF-CCS signal failure along fault-tolerant algorithm reliability for case 3.

cation of HR-SDN network communication in the NPP digital safety feature control system when a certain degree of fault-tolerant algorithm coverage for the HR-SDN communication module is guaranteed. For instance, the risk effect of data communication failure on ESFAS generation unavailability is estimated to be 13.81% when a coverage of 0.99 is achieved for both fault detection and fault recovery algorithms, which results in both higher network reliability and lower risk effect of network failure on system unavailability, compared to HR-SDL system.

5. Conclusion

The ESF-CCS, which employs a data communication system for the transmission of safety-critical signals from GCs to the LCs, was developed to effectively accommodate a vast number of field controllers. However, application of the developed ESF-CCS in NPPs has faced challenges regarding regulatory requirements for safety-related digital systems because the risk effects of data communication failure on the overall plant risk have not yet been completely quantified. In this study, fault tree models for the HR-SDL and HR-SDN systems were developed considering the interconnection between communication modules in each system and their hazard states and failure paths in the ESF-CCS in order to quantify the unavailability of safety-critical signal generation due to communication failure.

The developed fault tree model was applied to several case studies to assess the risk effects of communication failure between the GCs and LCs on ESF-CCS signal failure, and the related MCSs regarding ESFAS generation unavailability were identified. The quantification results indicated that the HR-SDL system achieves higher reliability than the HR-SDN system having a single network channel, since the failure of an LC communication module was the main contributor to communication failure in both cases, while the HR-SDL module has lower module unavailability than the HR-SDN module. In case of the HR-SDN system having a redundant network

channel, the unavailability of ESFAS generation due to network failure was much lower because the CCF of the communication modules was the dominant factor in determining ESFAS unavailability, and the redundancy of the network channel reduces the effect of network module failure in a single channel by a factor of the fault coverage of the fault-tolerant algorithms.

Since the fault-tolerant algorithms play an important role in terms of network risk for the HR-SDN system, sensitivity studies were conducted by considering a wide range of fault coverages of the fault-tolerant algorithms. Results showed that the risk effect of communication failure on ESFAS unavailability decreases from 28.37% to 13.81% when the fault coverages of the fault-tolerant algorithms are assumed as 0.7 to 0.99, respectively. This revealed the potential applicability of the HR-SDN system having a redundant network channel in terms of communication risk compared to the HR-SDL system when a certain degree of fault-tolerant algorithm coverage can be achieved.

Note that the ESF-CCS is a newly developed system with detailed design and component configuration yet unfixed; thus, the results discussed in this study may not be comparable with the results of other ESF-CCS studies. This work is expected to provide an insight into the reliability assessment of safety-critical data communication in NPP digital I&C systems. In future research, the fault tree model and assumptions used in the case studies can be employed as a basis for the development of a fault tree model after a detailed ESF-CCS design is prepared.

Based on the MCS analysis, the coverage of the fault-tolerant algorithm and network software failure probability are considered as important factors in the risk assessment of safety-critical network communication in ESF-CCS. Therefore, the detailed coverage of the HR-SDN fault detection and recovery algorithm and network software failure probability will also be investigated in order to assess the network risk in a more precise manner.

In addition to these factors, the risk effects of data communication failure in the ESF-CCS on the overall plant risk can be estimated by considering ESF components actuated via ESF-CCS in various ESF signal actuation conditions, and analyzing the system-level failure modes and causes of data communication in ESF-CCS based on the detailed functional allocation of LC and the field components in each division. Along with the modeling of automatic signal generation via safety-critical data communication in the ESF-CCS, the relationships among human action failures for the field components can be investigated based on condition-based human reliability assessment method to consider multiple human error conditions, since the ESF-CCS provides multiple manual actuation measures to assure system diversity (Kang and Jang, 2006).

Acknowledgements

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP:Ministry of Science, ICT and Future Planning) (NRF-2015M2A8A4021648).

References

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. Int. J. Hydrogen Energy 35 (3), 966–977.

Aldemir, T., 2006. Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria For Nuclear Power Plant Assessments. NUREG/CR-6901. US Nuclear Regulatory Commission, Washington DC, USA.

Aldemir, T., 2007. Dynamic Reliability Modeling of Digital Instrumentation and Control Systems For Nuclear Reactor Probabilistic Risk Assessments. NUREG/CR-6942. US Nuclear Regulatory Commission, Washington DC, USA.

Authen, S., Holmberg, J.E., 2012. Reliability analysis of digital systems in a probabilistic risk analysis for nuclear power plants. Nucl. Eng. Technol. 44 (5), 471–482.

Berghmans, F., Eve, S., Held, M., 2008. An introduction to reliability of optical components and fiber optic sensors. In: Optical Waveguide Sensing and Imaging. Springer, Netherlands, pp. 73–100.

Brown, S., 2000. Overview of IEC 61508 design of electrical/electronic/programmable electronic safety-related systems. Comput. Control Eng. J. 11 (1), 6–12.

Choi, J.G., 2007. Reliability Analysis Report of Safety Grade Programmable Logic Controller (POSAFE-Q). KNICS-PLC-AR103 Rev. 01. Korea Atomic Energy Research Institute, Daejeon, Republic of Korea.

Choi, K.C. et al., 2008. Design of high reliable safety data link (HR-SDL) for safety grade PLC (POSAFE-Q) for nuclear power plants. In: Proceedings of the 17th World Congress The International Federation of Automatic Control, Seoul, Korea, July 6–11.

Chu, T.L., 2008. Traditional Probabilistic Risk Assessment Methods for Digital Systems. NUREG/CR-6962. US Nuclear Regulatory Commission, Washington DC.

Dugan, J.B., Kishor, S.T., 1989. Coverage modeling for dependability analysis of fault-tolerant systems. IEEE Trans. Comput. 38 (6), 775–787.

Han, S.H., Lim, H.G., Yang, J.E., 2008. AIMS-PSA: a software for integrating various types of PSAs. In: International Probabilistic Safety Assessment and Management Conference. China, Hong Kong, pp. 18–23.

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. IEEE, pp. 187–192.

Hur, S. et al., 2013. The fault tolerant evaluation model due to the periodic automatic fault detection function of the safety-critical I&C systems in the nuclear power plants. Trans. Korean Inst. Electric. Eng. 62 (7), 994–1002.

Irwin, J.D., 1997. The Industrial Electronics Handbook. CRC Press.

Jian, S., Shaoping, W., 2006. Reliability analysis and congestion control on network nodes. In: IEEE Conference on Robotics, Automation and Mechatronics. IEEE, pp. 1–6.

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. Reliab. Eng. Syst. Saf. 91 (6), 627–633.

Kang, H.G., Jang, S.C., 2008. A quantitative study on risk issues in safety feature control system design in digitalized nuclear power plant. J. Nucl. Sci. Technol. 45 (8), 850–858.

Kang, H.G. et al., 2009. An overview of risk quantification issues for digitalized nuclear power plants using a static fault tree. Nucl. Eng. Technol. 41 (6), 849–858.

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). In: Transactions of the Korean Nuclear Society Spring Meeting, Jeju, Korea, May 10–11.

Kisner, R. et al., 2007. Safety and Nonsafety Communications and Interactions in International Nuclear Power Plants. Oak Ridge National Laboratory, United States.

Lee, J.S. et al., 2006. Evaluation of error detection coverage and fault-tolerance of digital plant protection system in nuclear power plants. Ann. Nucl. Energy 33 (6), 544–554.

Lee, D.Y., Lee, C.K., Hwang, I.K., 2008. Development of the Digital Reactor Safety System. KAERI/RR-2914/2007. Korea Atomic Energy Research Institute, Daejeon, Republic of Korea.

Lee, C.H., 2013. Development of Safety Evaluation Techniques for Digital I&C System using Test Platform, KINS/RR-1023. Korea Institute of Nuclear Safety.

Lee, S.J., Kim, M.C., Jung, W.D., 2014. Experimental Approach to Evaluate the Reliability of Digital I&C Systems in Nuclear Power Plants, Probabilistic Safety Assessment and Management (PSAM 12). Honolulu, Hawaii.

Lee, S.H. et al., 2015. Reliability modeling of safety-critical network communication in a digitalized nuclear power plant. Reliab. Eng. Syst. Saf. 144, 285–295.

Lim, T.J., Park, S.G., Seo, S.J., 2006. A Study on Methodologies for Assessing Safety Critical Network's Risk Impact on Nuclear Power Plant, KAERI/CM-989/2006. Korea Atomic Energy Research Institute, Daejeon, Republic of Korea.

Park, H.S., Oh, H., Park, W.J., 2008. Study on the High Reliable Communication for Hard Real Time Environment. KAERI/CM-1078/2007. Korea Atomic Energy Research Institute, Daejeon, Republic of Korea.

Willig, A., Wolisz, A., 2001. Ring stability of the PROFIBUS token-passing protocol over error-prone links. IEEE Trans. Industr. Electron. 48 (5), 1025–1033.