RISK ASSESSMENT OF SAFETY-CRITICAL DATA COMMUNICATION IN DIGITAL SAFETY FEATURE CONTROL SYSTEM

Sang Hun Lee, and Hyun Gook Kang
Department of Mechanical, Aerospace, and Nuclear Engineering
Rensselaer Polytechnic Institute
110 8th St, Troy, NY, USA
lees35@rpi.edu; kangh6@rpi.edu

Won Dae Jung, and Kwang Seop Son
Korea Atomic Energy Research Institute
111, Daedeok-daero, Daejeon, Republic of Korea
wdjung@kaeri.re.kr; ksson78@kaeri.re.kr

ABSTRACT

As one of the safety-critical systems in Advanced Power Reactor-1400 (APR-1400) nuclear power plant (NPP), the Engineered Safety Feature-Component Control System (ESF-CCS) employs safety data link and network communication for transmitting safety component actuation to effectively facilitate various safety-critical field controllers. However, data communication failure risk in the ESF-CCS has yet to be fully quantified, the probability that a safety-critical system in digitalized NPP becomes unsafe due to a network failure must be evaluated to quantify the risk of digital I&C system. In this study, a fault tree model was developed to assess the data link and data network failure-induced unavailability of a safety-critical system function used to generate an automated control signal for actuating design basis accident mitigation equipment. Especially, the risk of data communication failure in a digital safety feature control system was analyzed in consideration of interconnection between safety-critical controllers and the fault-tolerant algorithm implemented in the network configuration. Based on the developed fault tree model, case studies were performed to quantitatively assess the unavailability of ESF-CCS signal generation due to safety data link and network failure and their risk effect on safety signal generation unavailability. This study is expected to provide risk information on the safety-critical data communication in a digitalized NPP instrumentation and control system.

Key Words: Nuclear Power Plant; Digital I&C System; Safety Data Communication; Probabilistic Risk Assessment

1 INTRODUCTION

In analog instrumentation and control (I&C) systems for nuclear power plants (NPPs), most connections between controllers are comprised of point-to-point hard-wired types. Since they are based on analog technologies, they are fragile to noise and require analog-to-digital conversion time. Therefore, I&C systems in NPPs have recently been replaced with digital-based systems. Especially, interconnections between programmable logic controllers (PLCs) in digital I&C systems have been employed to supplant conventional hard-wired signal transmission. The interconnections are often based on data communication protocol which allows effective data transmission between PLCs for conducting multiple operational functions, including safety-critical functions.

For communication standards used for such NPP safety-critical applications, the commercial protocols were 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. 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 becomes unavailable due to data communication failure must be assessed to address the communication risk into the system unavailability and the plant risk.

Previous studies conducted on the risk assessment of data communication used for NPP safety-critical digital applications concerned a deterministic reliability assessment of a token ring protocol, which is a widely used protocol for controlled channel access in NPPs [1]. Relatively few studies though have been performed to assess communication failure risk and to analyze its risk effects on the NPP safety-critical systems [2-4]. In one previous study, data transmission 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 [2]. A limitation in the treatment of network communication protocol failure in this approach 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 fault-tolerant algorithm are employed to detect the network faults, 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 [3, 4]; limitations though of such dynamic modeling methods for data communication include the difficulty in integrating the model into a conventional plant risk model which incorporates human errors related to digital systems, as well as the digital equipment failures and their CCFs.

Therefore, a proper probabilistic risk assessment (PRA) framework for assessing the reliability of a safety communication system should be developed by considering network characteristics, such as its protocol and architecture in the safety-critical application. In this study, the reliability of a safety data link and network communication applied between group controllers (GCs) and loop controllers (LCs) in the Engineered Safety Feature-Component Control System (ESF-CCS) [5] developed by Korea Atomic Energy Research Institute (KAERI) is assessed. Especially, a fault tree model of signal generation failure of an engineered safety feature (ESF) component failure is developed 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 and the developed model integrated into a plant risk model. Based on the case studies and cut set analysis, the risk effect of network failure on plant risk and the important risk contributors of network failure were quantitatively addressed.

2 TARGET SYSTEM

As one of the safety-critical system of the Advanced Power Reactor-1400 (APR-1400) man-machine interface system (MMIS), the ESF-CCS was developed to effectively accommodate the field controllers which are actuated to conduct the safety-critical function in case of NPP DBA. The functions of the digital engineered safety feature actuation system (DESFAS) 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 facilitate the huge number of field controllers connected to 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), have been employed for the transmission of safety-critical information from GCs to LCs.

2.1 High Reliability-Safety Data Link Communication

The HR-SDL is a safety-graded communication module for transmitting safety-critical signals, and it uses the Profibus-Fieldbus Data Link (Profibus-FDL) based on send data with no acknowledge (SDN). It uses deterministic protocol to secure real-time operation and unidirectional peer-to-peer communication methods to only communicates through a dedicated fiber-optic link between two communication modules which allows physical isolation. In the ESF-CCS applied with HR-SDL, 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; thus, an optical splitter module (NFD1S-1Q) is used for 1-to-N communication between the GCs and LCs. The NFD1S-1Q converts the electrical signal received from the RS-485 transceivers module (NFD1-5Q) in the GC by RS-485 to four identical optical signals, which are separately transmitted to each fiber optic transceiver module (NFD1-6Q) in the LC located in the same division. The configuration of HR-SDL connections between a GC and four LCs in the same ESF-CCS division is shown in Fig. 1.

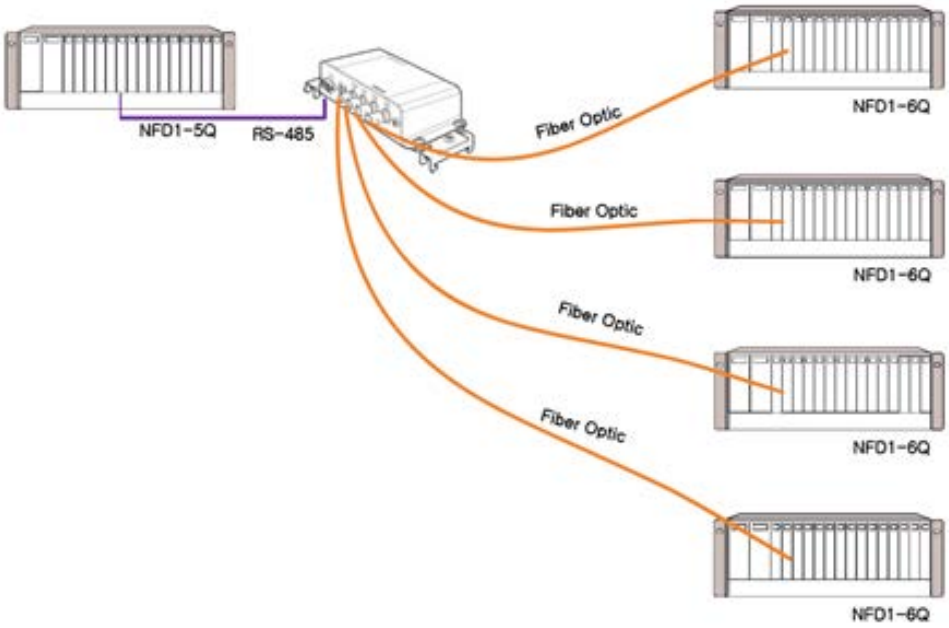

Figure 1. Interconnection between HR-SDL communication modules in the ESF-CCS.

2.2 High Reliability-Safety Data Network Communication

The HR-SDN also employs Profibus-FDL protocol based on SDN communication, however, HR-SDN physically follows a bus topology. Using shared network bus medium, HR-SDN communication module provides N-to-N safety-critical data exchange through network buses between safety-graded PLCs. Compared to the HR-SDL based on peer-to-peer connection, redundant network modules and buses are implemented in the HR-SDN system for the diversity in order to ensure reliable ESF actuation signal transmission in the ESF-CCS, as shown in Fig. 2 [6]. In each division, there are doubly redundant network channels, e.g. Primary NET and Standby NET, connected to the HR-SDN modules. 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.

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 [6]. That is, 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. The algorithm checks whether all data is received by the network module 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.

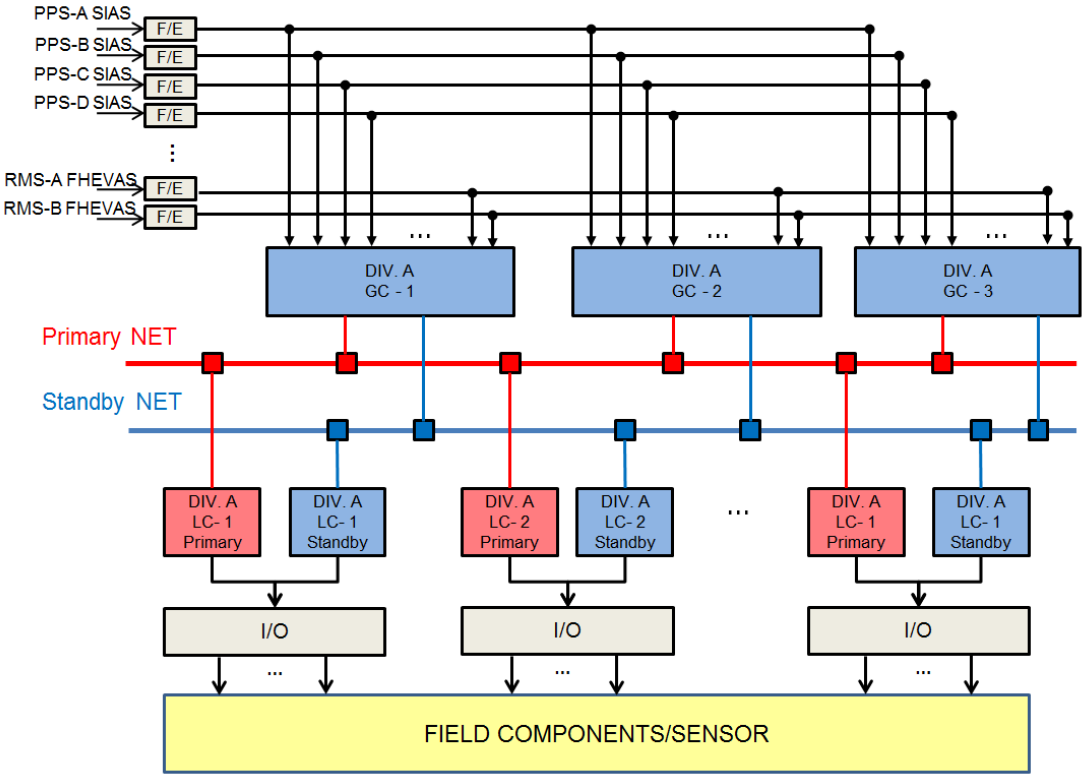

Figure 2. Configuration of the ESF-CCS applied with HR-SDN communication system.

3 MODEL DEVELOPMENT

The major safety-critical function of the ESF-CCS is to initiate emergency actuations in case of NPP DBAs. Therefore, the data communication failure results in the ESFAS generation failure for the ESF components via ESF-CCS. In this study, 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 related failure mechanisms, which were investigated in authors' previous research [7]. The fault tree is then 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.

3.1 Modeling of Network Failure Modes and Causes

ESF-CCS design is based on a PLC, which consists of various modules such as processor, digital input/output, and communication module. 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. Based on the auctioneering results, the GCs

transmit safety-critical information to the LCs in the same division, and then digital output modules in the LCs address automatic control signals to the relevant field components.

The HR-SDL communication module consists of two boards: the communication processor board (CPB) and the driver board (DRB). The CPB provides an interface between the processor module and the DRB, while the DRB is interfaced with the CPB and other PLCs through two communication ports. In case of HR-SDN, the communication 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. 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. In this study, the failure of communication module was modeled considering the failure of the hardware components and dedicated software functions in the module, and the token or data frame corruption caused by noise in the transmission medium.

3.2 Fault-tree Model Development for Network Risk Assessment

The top event of the system unavailability model in this study is the failure of corresponding ESFAS generation of a particular ESF component. The fault tree model of GC-LC communication failure is constructed based on the RM-ESFCCS, originally established by Kang et al. [2]. The model was further developed considering the detailed layout of each network system 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 controller, ESFAS-required safety components used for DBA mitigation measures are functionally allocated in the LCs of each division of the ESF-CCS.

Assuming that the ESF of the APR-1400 is the same as that of its predecessor OPR-1000, the ESF-CCS provides an initiation signal to each of the following independent ESF functions, such as the recirculation actuation signal (RAS). As an application of the proposed framework, a fault tree model for ESF-CCS signal failure was developed for the sump isolation valve SI-V675 in an RAS condition as a case study. 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.

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

The logic of the developed model for ESFAS generation failure in case of ESF-CCS applied with HR-SDL (comprising of data link based on peer-to-peer connection between communication modules) is shown in Fig. 3. 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. ESFAS failure can also be caused by the failure to provide input signals to the LC including data transmission failure between GCs and LC, and the failure of LC input signal generation by the GCs in the same division.

Since the LC receives the data frame regarding 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 failure due to transmission-medium-related bit errors in the received data frames from the three GCs in the same division. Failure to provide input to the LCs can 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 both independent failure and the CCF of the digital input/output and processor modules in the GC. The failure of the optical splitter module used for 1-to-N communication between GCs and LCs in the HR-SDL system is also modeled for each GCs in the same ESF-CCS division.

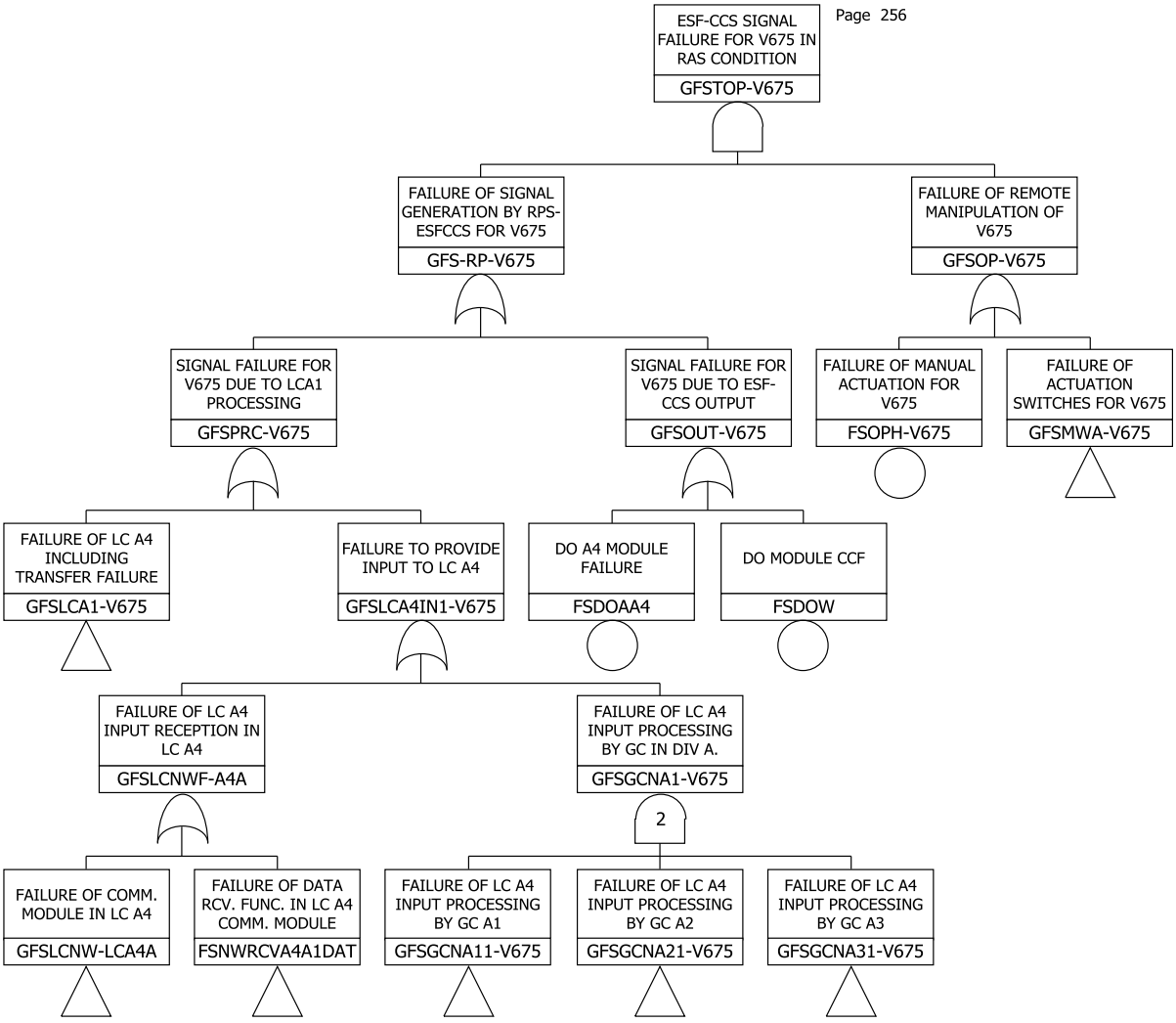

Figure 3. Top logic of ESFAS generation failure considering data communication failure in ESF-CCS with HR-SDL

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

The logic of the developed model for ESFAS generation failure of SI-V675 in case of the ESF-CCS with HR-SDN comprising a redundant network is shown in Fig. 4. 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 responsible for allowing the standby LC 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) considering redundant network channel.

Both HR-SDL and HR-SDN communication modules conduct the same safety-critical function, so the developed logic for HR-SDN network failure can be modeled in a similar manner as the HR-SDL model, where network failure in each LC includes both the failure of the HR-SDN module and the communication protocol. However, a redundant network bus structure is implemented in the HR-SDN network system, so the failure of network communication between the GCs and LCs is caused by the failure to provide input

to both the main and hot-standby backup LCs. In addition, the fault-tolerant algorithm is implemented in the HR-SDN protocol for reliable data transmission utilizing the redundant channel. The combination of a failure of the fault-tolerant algorithm, which includes both fault detection and removal algorithms, with the failure of a single network channel may cause a fault detection failure in the failed network channel, resulting in the failure to provide input to LCs by GCs in the same division. Therefore, the failure of both network fault detection and removal algorithms are also modeled as basic events in the developed fault tree model.

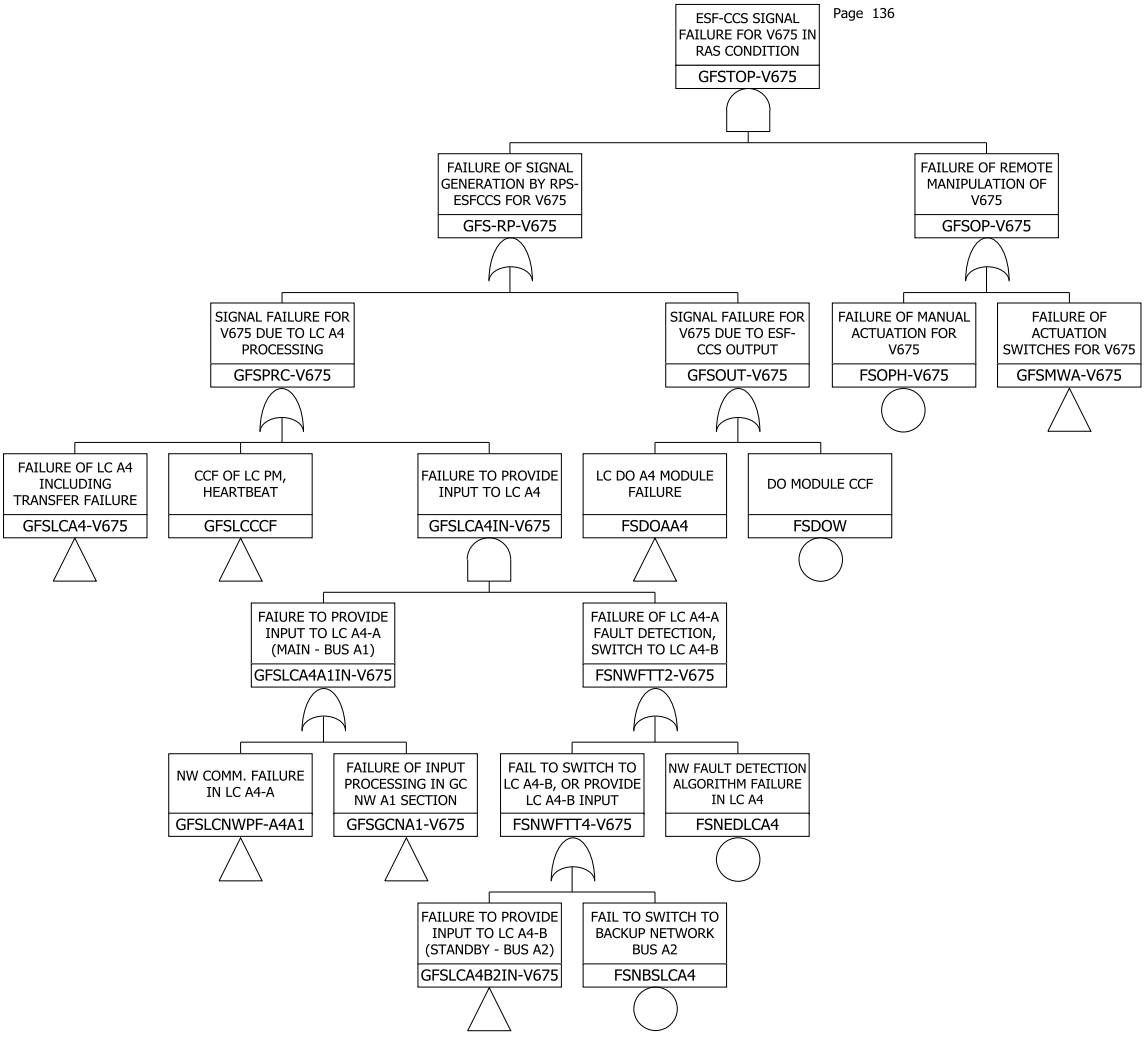

Figure 4. Top logic of ESFAS generation failure considering data communication failure in ESF-CCS with HR-SDN

4 RESULT

Based on the developed fault tree models for the ESF-CCS applied with HR-SDL and HR-SDN, the unavailability of ESF-CCS signal generation due to data link or data network failure and their risk effect on ESFAS generation failure was analyzed. In each case, the top event cutset was generated using the Advanced Information Management System for Probabilistic Safety Assessment (AIMS-PSA), 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. Based on varying ESF-CCS design specifications, risk quantification was performed and the related basic events related to network failure were analyzed 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-tolerant algorithm implemented for data network communication between GCs and LCs in the ESF-CCS

Since the ESF-CCS is a newly developed system and the detailed fault coverage or reliability of the fault-tolerant algorithms implemented for the HR-SDN network system was yet evaluated, the failure probability of both the fault detection algorithm by checksum and the fault removal algorithm for reconfiguring the HR-SDN network path when network fault is detected were assumed to be 0.7 as a case study based on Lee et al. [8].

4.1 Signal Unavailability due to Communication Failure

Based on the MCS analysis, the unavailability of ESFAS generation for SI-V675 in RAS and related data communication risk were quantified. Table I shows the summary of the quantification results for each case. The analysis result showed 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.

Table I. Quantification results of ESFAS unavailability considering network risk

	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	6.59e-05	6.95e-05	2.70e-05
Unavailability of ESFAS generation due to network failure	9.37e-06	1.29e-05	8.63e-06

4.2 Risk Effect of Network Failure on Safety Signal Unavailability

The network risk quantification result showed that the fault coverage of the fault-tolerant algorithms is one of the most important factor which determines ESFAS generation unavailability due to network

failure for the HR-SDN system having a redundant network channel. In this study, the effect of fault-tolerant algorithm failure on the reliability of the HR-SDN network system was analyzed by conducting sensitivity study on the fault coverage of such fault-tolerant algorithm ranging from 0.7 to 0.99. The risk effect of network failure on ESFAS unavailability at various fault coverage is shown in Fig. 5.

In result, the quantification results for both network protocols applied in the ESF-CCS revealed the potential application 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 14.09% for the fault detection coverage (C_1) of 0.93 at the coverage of fault recovery algorithm (C_2) of 0.99, and 13.66% for C_1 of 0.98 at C_2 of 0.95, which results in both higher network reliability and lower risk effect of network failure on system unavailability, compared to HR-SDL system (14.22%) as shown in Table I.

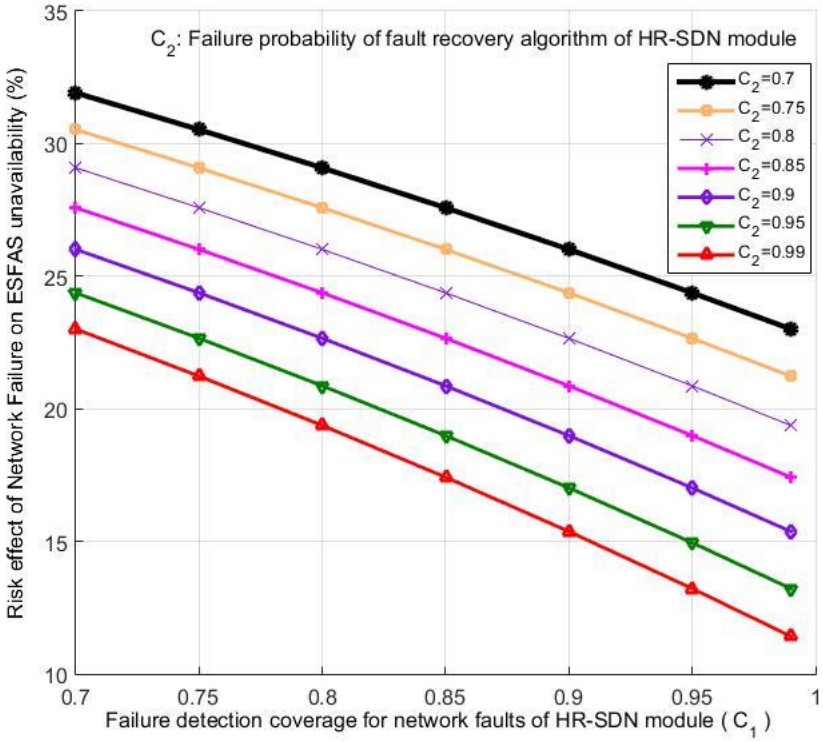

Figure 5. Risk effects of network failure on ESF-CCS signal failure at various fault-tolerant algorithm reliability.

5 CONCLUSIONS

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. In case of the HR-SDN system having a redundant network channel, the unavailability of ESFAS generation due to network failure was much lower compared to HR-SDL 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. The results 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 here can be employed as a basis for the development of an integrated fault tree model after the detailed ESF-CCS design including the detailed fault coverage of the fault-tolerant algorithms for the HR-SDN system is investigated.

6 ACKNOWLEDGMENTS

This work was supported by Nuclear Research & Development Program of the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (Grant Number: 2015M2A8A4021648)

7 REFERENCES

1. A. Willig, and A. Wolisz., "Ring stability of the PROFIBUS token-passing protocol over error-prone links," *IEEE Transactions on Industrial Electronics*, **48.5**, pp.1025-1033 (2001).
2. H. G. Kang, and S. C. Jang., "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**, pp.850-858, (2008).
3. A. W. Al-Dabbagh, and L. Lu., "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**, pp.966-977, (2010).
4. S. Jian, and W. Shaoping, "Reliability analysis and congestion control on network nodes," *Robotics, Automation and Mechatronics, 2006 IEEE Conference on.,* IEEE, (2006).
5. D. Y. Lee, C. K. Lee, and I. K. Hwang., *Development of the digital reactor safety system*, Korea Atomic Energy Research Institute, Republic of Korea (2008).
6. T. J. Lim, et al., *A Study on methodologies for Assessing Safety Critical Network's Risk Impact on Nuclear Power Plant,* Korea Atomic Energy Research Institute, Republic of Korea (2007).
7. S. H. Lee, et al. "Reliability modeling of safety-critical network communication in a digitalized nuclear power plant," *Reliability Engineering & System Safety*, **144**, pp.285-295 (2015).
8. J. S. Lee, et al. "Evaluation of error detection coverage and fault-tolerance of digital plant protection system in nuclear power plants," *Annals of Nuclear Energy*, **33.6**, pp.544-554 (2006).