Reliability Assessment of Safety-Critical Network Communication in a Digitalized Nuclear Power Plant

Sang Hun Lee, Hyun Gook Kang*

[1]*Department of Nuclear and Quantum Engineering, KAIST, Yuseong-gu, Daejeon, 305-701, Republic of Korea*
*titanic91@kaist.ac.kr; *hyungook@kaist.ac.kr*

INTRODUCTION

In analog instrumentation and control (I&C) systems for nuclear power plants (NPPs), most connections are comprised of hardwired point-to-point types. Since they are based on analog technologies, they are fragile to noise and require analog-to-digital conversion time. Therefore, many NPPs have adopted communication network for the exchange of safety-critical data between programmable logic controllers (PLCs) in digital I&C systems to effectively accommodate a huge number of field controllers [1]. However, the primary issue of digital network communication in a safety-critical system involves potential hazards, such as partial or total loss of communication between PLCs, which may result in a failure of safety-critical signal generation when it is needed [2, 3]. Therefore, 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 Korea, the Engineered Safety Feature-Component Control System (ESF-CCS) was developed as one of the digital safety-critical system in Advanced Power Reactor-1400 (APR-1400) [4]. The function of a digital engineered safety feature (ESF) actuation system and field actuator controllers of conventional NPPs are performed by the ESF-CCS. In this system, safety-critical network, High Reliable-Safety Data Network (HR-SDN), was employed for the safety-critical data transmission from group controllers (GCs) to loop controllers (LCs), as shown in Fig 1.

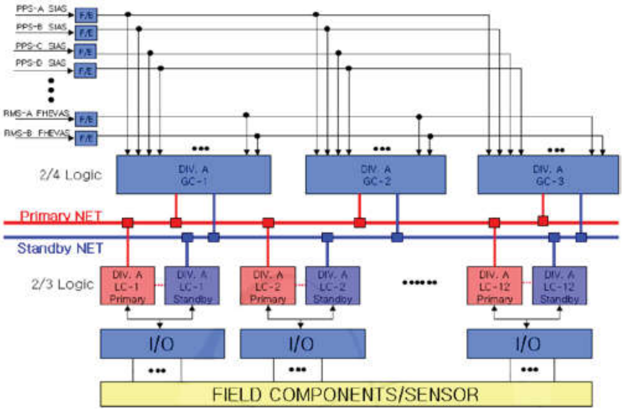

Fig. 1. Configuration of GCs and LCs in ESF-CCS [4]

In this study, a framework for assessing the reliability of a HR-SDN network communication between GCs and LCs in the ESF-CCS in addition to a fault-tree model for ESF components considering network failure between GCs and LCs were developed to assess the plant risk effect of a newly developed digitalized ESF-CCS. 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.

TARGET SYSTEM

High Reliable-Safety Data Network in ESF-CCS

The ESF-CCS initiates various emergency actuation signals to prevent a plant from entering a hazardous state during and/or after an accident [4]. When the ESF initiation signals are generated and transmitted to the ESF-CCS, automatic ESF actuation signals are sent to corresponding field components such as pumps and valves. To effectively accommodate the vast number of field components in a plant, a HR-SDN system is employed in ESF-CCS loop control network, which is used for the transmission of safety-critical data from the GCs to the LCs.

HR-SDN communication module consists of a communication CPU (XC161CJ) and a driver CPU (DsTni-LX). Software implemented in communication CPU and driver CPU is called PNOS4 and PNIOS4, respectively. The communication module is interfaced through 8 bits bus with the processor module and both CPUs are accomplished in a single board where driver CPU supports a single communication port, as shown in Fig. 2 [5].

In terms of operation mechanism, HR-SDN uses a Profibus-DP protocol based on send data with no acknowledge communication [4]. The operating mechanism of the Profibus-DP protocol used for HR-SDN

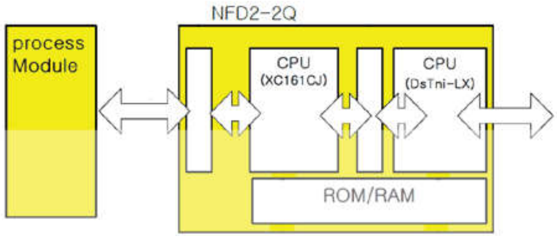

Fig. 2. Configuration of HR-SDN module [5]

communication is similar to that of the token bus protocol, which is specified in IEEE 802.4 [6].

MODEL DEVELOPMENT

Identification of Hazardous States and Failure Mechanisms

The operation mechanism of the Profibus-DP protocol can be categorized into four major processes: token frame reception, data frame transmission, data frame reception and token frame passing [6]. 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 failure causes, isolating errors, which are the errors that can be isolated to a given fault domain, namely, a station, its upstream neighbor, and the bus connection between them, were considered as the main failure causes for the Profibus-DP protocol in this study. For HR-SDN system, the functions specified in the Profibus-DP protocol are performed by hardware components and software functions in network modules of the GCs and LCs in the ESF-CCS. Thus, the failure causes of network communication can be categorized into hardware failure, software failure, and the failure caused by medium-related bit errors. Table I lists the identified hazardous states and failure causes of a target network communication system.

Table I. Summary of the Identified Hazardous States and the Failure Mechanisms

Hazardous States	Failure Mechanisms
Token reception failure	- Failure of network interface module of station - Failure of receiver in network module of station - Failure of software function in network module of station - Token frame corruption caused by bit errors in medium
Data transmission failure	- Failure of network interface module of station - Failure of transmitter in network module of station - Failure of software function in network module of station
Data reception failure	- Failure of network interface module of station - Failure of receiver in network module of station - Failure of software function in network module of station - Data frame corruption caused by bit errors in medium
Token passing failure	- Failure of network interface module of station - Failure of transmitter in network module of station - Failure of software function in network module of station

Quantification of Network Failure Probability

To estimate the risk effects of network communication failure between the GCs and LCs on ESF-CCS signal failure in ESF initiation conditions, a quantification scheme for each identified failure mechanism was proposed.

Quantification of Hardware Failure Probability

The HR-SDN system adopted for the network communication between the GCs and LCs is based on a safety-grade PLC [5]. A PLC consists of various modules, including an input module, a processor module, an output module and network modules [4]. Based on PLC module data shown in Table II, the failure probability of hardware modules were estimated based on Equation (1) [7].

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

Table II. Failure Rate of GC and LC Modules [4]

Component	Modules	Failure Rate (/hr)
GC	Power Supply	2.15E-05
	Processor	7.75E-06
	Digital Input	6.25E-06
	Base board	0.98E-06
	Comm. Processor (CP)	4.85E-06
	Comm. Driver (DR)	7.99E-06
LC	Power Supply	2.15E-05
	Processor	7.75E-06
	Analog Input	4.06E-06
	Analog Output	4.06E-06
	Digital Input	6.25E-06
	Digital Output	5.93E-06
	Base Board	0.98E-06
	Comm. Processor (CP)	4.85E-06
	Comm. Driver (DR)	7.99E-06

Quantification of Software Failure Probability

In terms of software failure probability quantification, a qualitative approach based on software integrity level was adopted in this study. For the software in HR-SDN module, as shown in Table III, software used in GC and LC in ESF-CCS, which is one of safety-graded I&C system in NPP, is regarded as safety-critical; thus, the software integrity level (SIL) of the software used in network modules in GC or LC is derived as SIL-4. Therefore, software failure probability of a SIL-4 target based on IEC 61508, which provides reliability targets for the safety software functions operating in the low demand mode of operation according to SIL, was applied as a software failure probability of HR-SDN module was modeled in the fault-tree model in this study [8, 9].

Table III. Software Specification of HR-SDN Module [4]

Software	Software Function	Safety Grade
PNOS4	- Data exchange between CP and processor - Data exchange between CP and DR - Error management for CPB, DRB - LED display	Safety-Critical
PNIOS4	- Data exchange between stations - Data exchange between PNIOS4 - Error management for DRB - LED display	Safety-Critical

Quantification of Failure Probability caused by Bit Error

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 safety-critical data in ESF-CCS which may result in hazardous states can be treated as the probability of failure on demand. In this study, the bit error rate (BER) was used to assess ESF-CCS signal generation failure probability due to medium-related bit error. The BER of Profibus physical layer is generally in the order of 1.0E-08 [10]. In this study, the estimated expected number of erroneous bits in token or data frame was treated as the probability of each frame corruption caused by bit errors introduced by the bus medium.

Fault-tree Modeling of HR-SDN Network Communication in ESF-CCS

ESF-CCS has four redundant channels, where each channel is equipped with triple redundant GCs and double redundant LCs, as shown in Fig. 3 [11]. The network medium also has a double redundant structure, where each network medium transmits a data frame from three GCs to each LC for the actuation signal of ESF components.

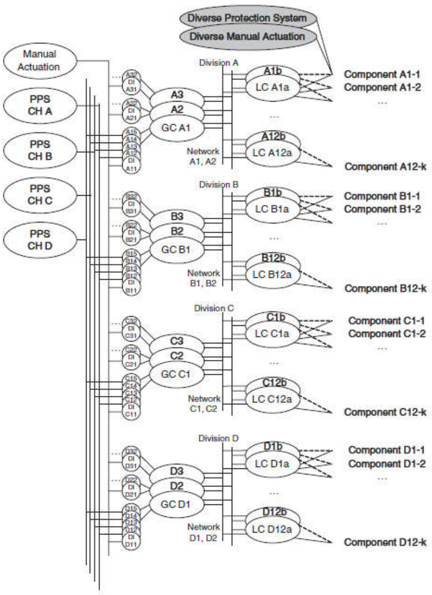

Fig. 3. Layout and signal flow of the ESF-CCS [11]

For the functional diversity of ESF-CCS, various safety-critical field controllers related to ESF actuation signals are functionally allocated to the LCs in four redundant channels in the ESF-CCS. In each division, the safety functions are also functionally allocated in each LC. Table IV shows the example of functional allocation of LCs for specific field controllers.

Table IV. Example of ESF Functional Allocation to LC

ESFAS	ESF	Description	LC Allocation
RAS-A	V675	Sump Iso v/v SI-V675	LC A4
	HX-1A	Spray Hx. inlet Iso. v/v V141	LC C4
SIAS-A	HP02A	HPSI pump SI-PP02A	LC A5
	LP01A	LPSI pump SI-PP01A	LC A6
	V637	Iso. v/v SI-V637	LC C5
	V647	Iso. v/v SI-V647	LC C6

Based on the identified hazardous states and failure mechanisms that may cause a network failure between GCs and LCs in the ESF-CCS, 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). A fault-tree model was developed for the ESF-CCS signal failure for a total of 36 ESF components required for various mitigation actions NPP design basis accidents (DBAs). Fig. 4 shows the logic of a developed model for ESF-CCS signal failure considering network failure for SI-V675 in RAS condition. It is notable that fault-tree model for other ESF components can be modeled in a same manner.

Since the human operator could also manually actuate the field components as a backup, the failure of remote manual actuation of ESF components was modeled. In this study, the failure probability of the human operator for manual actuation of ESF signal generation via diverse protection system was assumed as 0.05 and that of the field component via diverse manual actuation switch is assumed as 0.1 based on the conventional human error probability (HEP) method [11]. In addition, the failure of multiple identical components in HR-SDN module, or common cause failure (CCF) of hardware modules, was considered by assuming the beta factor to be one tenth, based on the beta factor model [11].

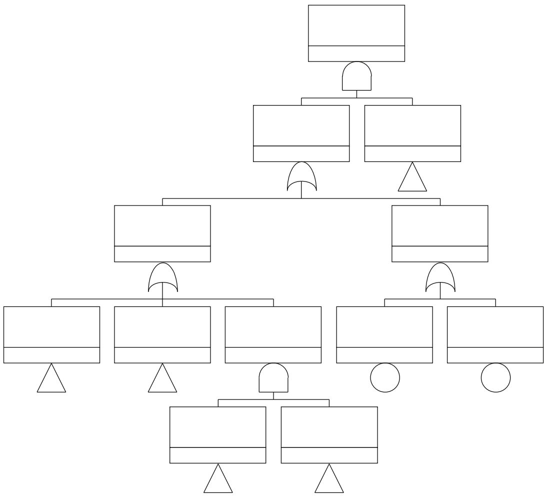

Fig. 4. Logic of a developed fault-tree model of the ESF-CCS (ESF-CCS signal failure for V675; GFSTOP-V675)

RESULTS

Sensitivity Study

To improve the reliability of digital I&C systems, testing strategies, including manual testing and automatic periodic testing, have been generally adopted. 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 HR-SDN module and their test intervals in this study. The detailed description of assumed test methods and their test interval is shown in Table V.

Table V. Description of Sensitivity Study Cases

Case	Test Method	Periodic Test Interval
1	Manual testing	730 hours
2	Automatic periodic testing by ETIP	8 hours
3	Automatic periodic testing by PLC self-diagnostics	50 milliseconds

In each case study, the minimal cut set for the top event, which is Small-LOCA core damage (CD) sequence was generated using the AIMS-PSA and the risk effect of network failure between the GCs and LCs on the Small-LOCA CD frequency was assessed. The quantification results showed that overall risk of network communication failure between GCs and LCs in ESF-CCS contributed up to 1.58% when manual testing for network hardware components are assumed.

The quantification results also revealed the important basic events related to network failure that contribute to the Small-LOCA CD frequency. For case 1, where manual testing is assumed, the hardware failure of the network modules was analyzed as an important failure mechanism contributing to overall network failure in the ESF-CCS. For cases 3, where the automatic periodic testing performed by the PLC self-diagnostics is assumed, the failure of the software functions in the network module was regarded as a dominant factor which contributes to overall network failure in the ESF-CCS. In terms of important basic events in the dominant cut sets for ESF-CCS signal failure, the CCF of both network hardware modules and software were analyzed.

CONCLUSION

In this study, a framework for identifying the potential hazardous states of network communication in the ESF-CCS was proposed. In addition, 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. The fault-tree model of ESF-CCS signal failure for ESF components required for various mitigation actions regarding NPP DBAs was designed by considering the identified hazardous states of network failure that would result in a failure to provide input signals to the corresponding LC.

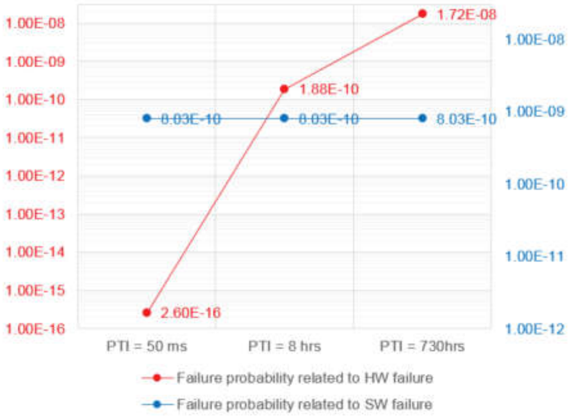

Fig. 5. Sensitivity study results for the effect of periodic test interval on network failure

As a sensitivity study, three case studies were performed based on the periodic test methods for hardware components in HR-SDN module and their test intervals in this study. The quantitative results for three case studies demonstrated that the probability of overall network communication failure, which was calculated as the sum of the failure probability associated with each failure cause, contributed up to 1.58% on the Small-LOCA CD frequency. The results also revealed the important basic events related to network failure in the case studies which included CCF of hardware and software in HR-SDN module.

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 data transmission in NPPs. As a further study, the risk effects of network failure in the ESF-CCS on the plant risk can be estimated in a more detailed manner by analyzing the failure modes and causes in a sub-component level and the fault detection coverage of the fault tolerance techniques for network failure implemented in ESF-CCS after the detailed configuration of ESF-CCS is decided. In terms of the failure of manual ESF actuation, 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 (CBHRA) method or the dynamic human reliability modeling approach 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 [12, 13].

ACKNOWLEDGEMENT

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)

REFERENCES

1. PRECKSHOT, G. G., and R. H. WYMAN. "Data Communication Systems in Nuclear Power Plants." Lawrence Livermore Nat. Lab., Livermore, CA (1993).

2. KISNER, R. A., et al. Safety and Nonsafety Communications and Interactions in International Nuclear Power Plants, TN, 2007.

3. KISNER, R. A. Design Practices for Communications and Workstations in Highly Integrated Control Rooms. US Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, 2009.

4. LEE, D. Y., C. K. LEE, and I. K. HWANG. Development of the digital reactor safety system. Korea Atomic Energy Research Institute, Daejeon (Korea, Republic of), 2008.

5. PARK, H. S., H. OH, and W. J. PARK. Study on the High Reliable Communication for Hard real time environment. Korea Atomic Energy Research Institute, Daejeon (Korea, Republic of), 2008.

6. IEEE, IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification, IEEE, New York, USA, 1985.

7. OHRING, Milton. Reliability and failure of electronic materials and devices. Academic Press, 1998.

8. AUTHEN, S., and J. E. HOLMBERG. "Reliability analysis of digital systems in a probabilistic risk analysis for nuclear power plants." *Nuclear Engineering and Technology*, **44**, 5, 471-482 (2012).

9. Brown, S. "Overview of IEC 61508 Design of electrical/electronic/programmable electronic safety-related systems," *Computing and Control Engineering Journal*, **11,** 1, 6-12 (2000).

10. IRWIN, J. D. The industrial electronics handbook. CRC Press, 1997.

11. KANG, H. G., 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, 850-858 (2008).

12. Kang, H. G., and S. C. Jang, "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 (2006).

13. Boring, R. L. "Dynamic human reliability analysis: Benefits and challenges of simulating human performance," *Risk, Reliability, and Societal Safety*, **2**, 1043-1049 (2007).