Fault-Tree Modeling of Safety-Critical Network Communication in a Digitalized Nuclear Power Plant

Sang Hun Lee [a] and Hyun Gook Kang [a*]
[a]Department of Nuclear and Quantum Engineering, KAIST, 291 Daehak-ro (373-1 Guseong-dong), Yuseong-gu, Daejeon, 305-701, Republic of Korea.
[*]*Corresponding author: hyungook@kaist.ac.kr*

1. Introduction

Recently, instrumentation and control (I&C) systems in nuclear power plants (NPPs) have been replaced with digital-based systems. Digital components provide improved performance in terms of accuracy and computational capabilities and have achieved higher data handling and storage capacities [1].

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

Previous studies have suggested that the risk effects associated with network protocol failures are important factors in determining the overall risk of a digital I&C system, especially in the case of the ESF-CCS; thus, the risk effects of network failures in the ESF-CCS must be analyzed to investigate the risk of the developed MMIS [3]. Therefore, a fault-tree model that can be used to analyze the risk effects of network communication failures on ESF-CCS signal failures for a target field component were developed in this study.

2. Target System

2.1 High Reliability-Safety Data Network

To effectively accommodate the vast number of field components in a plant, a high reliability-safety data network (HR-SDN) system is employed in ESF-CCS loop control network (ELCN), which is used for the transmission of safety-critical data from the GCs to the LCs [4]. The HR-SDN system uses the Profibus-DP protocol, which is based on send data with no acknowledge communication; this protocol is a standard fieldbus protocol that is extensively applied in other industry fields [5].

In terms of the operating mechanism of the Profibus-DP protocol, the protocol that is used for communication is similar to that of the token bus protocol [6]. The IEEE has established the IEEE 802.4 standard, which specifies the services and a standard for local area networks that use explicit token passing schemes to control access on a bus topology network [7].

3. Proposed Framework

3.1 Identification of Hazardous States and Failure Causes

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 [8]. 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, two types of failure causes exist in the Profibus-DP protocol: isolating errors and non-isolating errors [9]. Isolating errors are errors that can be isolated to a given fault domain, namely, a station, its upstream neighbor, and the wire between them. In this study, the isolating errors were treated as the main failure causes in the Profibus-DP protocol; thus, the causes of these errors were categorized into hardware failure, software failure and failure caused by medium-related bit errors.

Table I lists the identified hazardous states and failure causes of the target network communication system.

Table I: Summary of the identified hazardous states and the corresponding causes of failure

Hazardous States	Failure Causes
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 network 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

3.2 Fault-Tree Analysis of Network Communication in GCs and LCs

ESF-CCS has four redundant channels, where each channel is equipped with three redundant GCs and doubly redundant LCs. The network medium also has a doubly redundant structure, in which each network medium transmits a data frame from the three GCs to the corresponding LC for a specific safety component actuation signal. The fault-tree analysis of ESF-CCS signal failure in a certain ESF initiation condition was developed based on the configuration of the ESF-CCS, as shown in Fig. 1 for the case study.

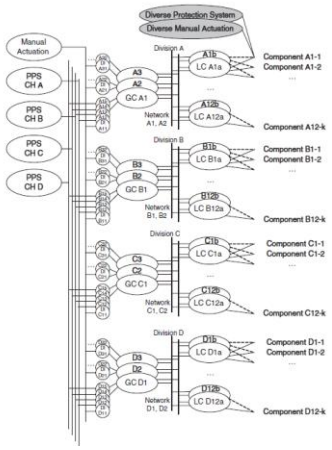

Fig. 1. Conceptual layout and signal flow of the ESF-CCS [3]

3.2.1 A Case Study: ESF-CCS signal failure for the containment spray pump in CSAS condition

A fault-tree model of GC-LC network communication failure was developed based on the RM-ESFCCS, which was originally developed by Kang et al. [3] based on the redundancy concept as well as the identified hazardous states and corresponding causes of failure regarding network communication between GCs and LCs. In the case study, a fault-tree model was developed for ESF-CCS signal failure for the containment spray (CS) pump PP01A in the CSAS condition as an example of the functional allocation of LCs in the CSAS condition. 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). The logic of the model is illustrated in Fig. 2.

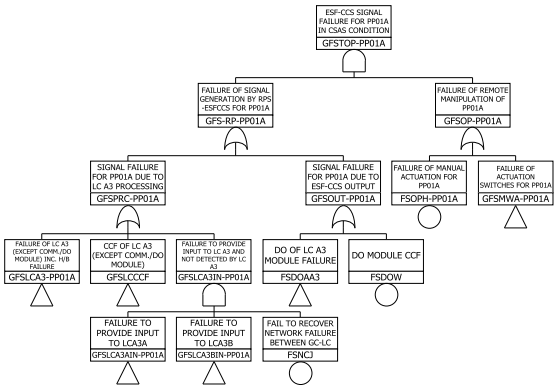

Fig. 2. Top logic of the developed fault-tree model of the ESF-CCS (CSAS-A signal failure for the field component PP01A; GFSTOP-PP01A)

In terms of network communication failure between the GCs and LCs, ESF-CCS signal failure for a CS pump in the CSAS condition can be caused by a failure to provide input to the corresponding LCs, which consist of the main LC and the hot standby backup LC. A failure to recover a network failure between the GCs and LCs can also lead to a failure to provide input to the corresponding LCs. As shown in Fig. 2, the top logic of the developed fault-tree model of ESF-CCS signal failure for a CS pump includes the failure of signal generation caused by the failure of signal processing by the LCs and the failure of the digital output module of the PLC in the ESF-CCS. The failure of manual actuation signals from diverse protection system (DPS) is also considered.

To estimate the risk effects of network communication failure on ESF-CCS signal-generation failure, the top-event cut sets were generated, and the risk effects of network communication failure between the GCs and LCs in the ESF-CCS were evaluated by analyzing the basic events related to network communication failure based on the dominant cut sets thus derived.

4. Results

4.1 Sensitivity Study

For the sensitivity four case studies were performed. The values adopted for the baseline software failure probability as well as the periodic inspection intervals for manual testing and the automatic periodic testing performed by the self-diagnostic function implemented in the PLC are summarized in Table II.

Table II: Summary of the identified hazardous states and the corresponding causes of failure

Description	Case 1	Case 2	Case 3	Case 4
Baseline software failure probability	1.0E-04	1.0E-05	1.0E-04	1.0E-05
Periodic inspection interval	730 hr	730 hr	50 ms	50 ms

In each case study, the top-event cut set was generated using the AIMS-PSA, and the risk effect was estimated for each cause of network communication failure between the GCs and LCs. As shown in Fig. 3, which presents the dominant cut sets of the developed fault tree for case 1, the important basic events in the dominant cut sets for ESF-CCS signal failure in case 1 related to the digital component unavailability include digital output module failure, the common cause failure of the network modules in the corresponding division, and loop controller module failure, among others. They affect the unavailability of the ESF-CCS signal generation in combination with the manual actuation failure by human operator.

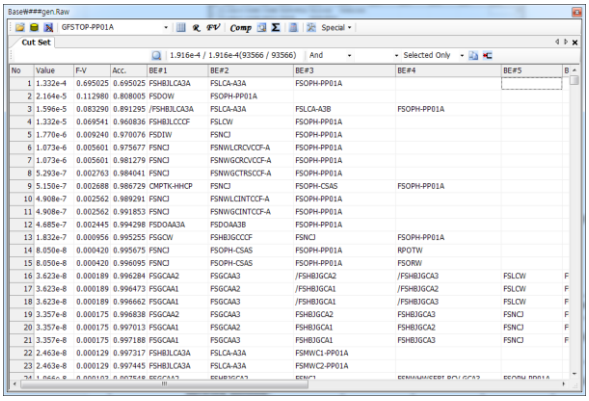

Fig. 3. Dominant top-event cut sets of the fault tree (CSAS-A signal failure for the field component PP01A; GFSTOP-PP01A) for case 1

The dominant cut sets for ESF-CCS signal failure in the other case studies were derived in a similar manner. Then, based on the analyzed top-event cut sets, the failure probability was estimated for each failure cause, including hardware failure, software failure and token or data frame corruption caused by network-medium-related bit errors.

4.2 Assessment of Risk Effect of Network Failure

Based on the quantification results for each failure cause in the four case studies, the risk effects of network failure on the top event were estimated. The results indicate that overall network communication failure — which was calculated as the sum of the failure probabilities of the hardware components; the probability of failure of software operation in the network module; and the probability of frame corruption in the network medium — contributes up to 1.88% of the probability of ESF-CCS signal failure for the CS pump considered in the case study.

5. Conclusions

A framework for identifying the potential hazardous states of network communication in the ESF-CCS was proposed, and a fault-tree model for network communication failure was developed to estimate the risk effects of network failure between the GCs and LCs on ESF-CCS signal failure. The developed fault-tree model was then applied to several case studies. As an example of the development of a fault-tree model for ESF-CCS signal failure, the fault-tree model of ESF-CCS signal failure for CS pump PP01A in the CSAS condition 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.

The quantitative results for four 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, contributes up to 1.88% of the probability of ESF-CCS signal failure for the CS pump considered in the case studies. To address the effect of using the digitally based ESF-CCS on the overall plant risk, the risk effects of network failure in the ESF-CCS on the CDF can be analyzed by expanding the developed fault-tree model, where the network failure risk was treated as an independent failure causing the loss of input to the LCs, to the network communication between the GCs and LCs under other ESF initiation conditions.

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: 2015M2A8A402164)

REFERENCES

[1] National Research Council. Digital Instrumentation and Control Systems in Nuclear Power Plants: safety and reliability issues. National Academy Press, DC, USA, 1997.
[2] Lee, Dong Young, et al. "Development Experiences of a Digital Safety System in Korea." IAEA Technical Meeting on the impact of Digital I&C Technology on the Operation and Licensing of NPP, Beijing, China, Nov. 2008.
[3] Kang, Hyun Gook, and Jang, Seung-Cheol. "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 (2008): 850-858.
[4] Kim, Seong Tae, et al. "New Design of Engineered Safety Features-component Control System to Improve Performance

and Reliability." 15th Pacific Basin Nuclear Conference, Sydney, Australia, Oct. 15-20 2006.
[5] Kim, Young Jin, et al. Design Support for ESF-CCS. Korea Atomic Energy Research Institute, Daejeon, Republic of Korea, 2008.
[6] Willig, Andreas, and Adam Wolisz. "Ring stability of the PROFIBUS token-passing protocol over error-prone links." Industrial Electronics, IEEE Transactions on 48.5 (2001): 1025-1033.
[7] IEEE, IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification, IEEE, New York, USA, 1985.
[8] Elahi, Ata. Network communications technology. Cengage Learning, 2001.
[9] Haugdahl, J. Scott. Network analysis and troubleshooting. Addison-Wesley Professional, 2000.