Reliability Engineering and System Safety 144 (2015) 285–295

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Reliability modeling of safety-critical network communication in a digitalized nuclear power plant

Sang Hun Lee [a], Hee Eun Kim [a], Kwang Seop Son [a,b], Sung Min Shin [a], Seung Jun Lee [c], 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
[b] I&C/Human Factors Research Division, Korea Atomic Energy Research Institute, 1045 Daedeok-daero, Yuseong-gu, Daejeon 305-353, Republic of Korea
[c] Integrated Safety Assessment Division, Korea Atomic Energy Research Institute, 1045 Daedeok-daero, Yuseong-gu, Daejeon 305-353, Republic of Korea

ARTICLE INFO

Article history:
Received 16 April 2015
Received in revised form
27 July 2015
Accepted 30 July 2015
Available online 11 August 2015

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

ABSTRACT

The Engineered Safety Feature-Component Control System (ESF-CCS), which uses a network communication system for the transmission of safety-critical information from group controllers (GCs) to loop controllers (LCs), was recently developed. However, the ESF-CCS has not been applied to nuclear power plants (NPPs) because the network communication failure risk in the ESF-CCS has yet to be fully quantified. Therefore, this study was performed to identify the potential hazardous states for network communication between GCs and LCs and to develop quantification schemes for various network failure causes. To estimate the risk effects of network communication failures in the ESF-CCS, a fault-tree model of an ESF-CCS signal failure in the containment spray actuation signal condition was developed for the case study. Based on a specified range of periodic inspection periods for network modules and the baseline probability of software failure, a sensitivity study was conducted to analyze the risk effect of network failure between GCs and LCs on ESF-CCS signal failure. This study is expected to provide insight into the development of a fault-tree model for network failures in digital I&C systems and the quantification of the risk effects of network failures for safety-critical information transmission in NPPs.

1. Introduction

Recently, instrumentation and control (I&C) systems in nuclear power plants (NPPs) have been replaced with digital-based systems. The reason for the transition to digital I&C systems lies in the critical advantages that they offer over conventional analog systems. Regarding conventional analog systems, certain design problems, such as issues related to the susceptibility to extreme environmental conditions, have been identified. The primary concerns associated with the extended use of analog systems, such as mechanical failure and environmental degradation, are related to the effects of aging. Digital electronic components provide improved performance in terms of accuracy and computational capabilities and have achieved higher data handling and storage capacities; thus, they allow operating conditions to be more thoroughly measured and displayed [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]. This system, which is illustrated in Fig. 1, is based on a network communication system for both intra-system and inter-system connections. However, because network communication failure risks in the MMIS architecture have not yet been fully studied and quantified, the application of this architecture to NPPs has been challenging because of issues related to the regulatory requirements for safety-related digital systems as well as communication-related requirements [3].

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 [4].

Regarding network communication failure, a previous study has demonstrated how to predict the failure of a commercial network system based on the likelihood of lost or delayed messages, using Ethernet and Echelon's LonTalk as examples, and the system failure rate associated with the loss of multiple consecutive messages was

* Corresponding author.
E-mail address: hyungook@kaist.ac.kr (H.G. Kang).

http://dx.doi.org/10.1016/j.ress.2015.07.029
0951-8320/

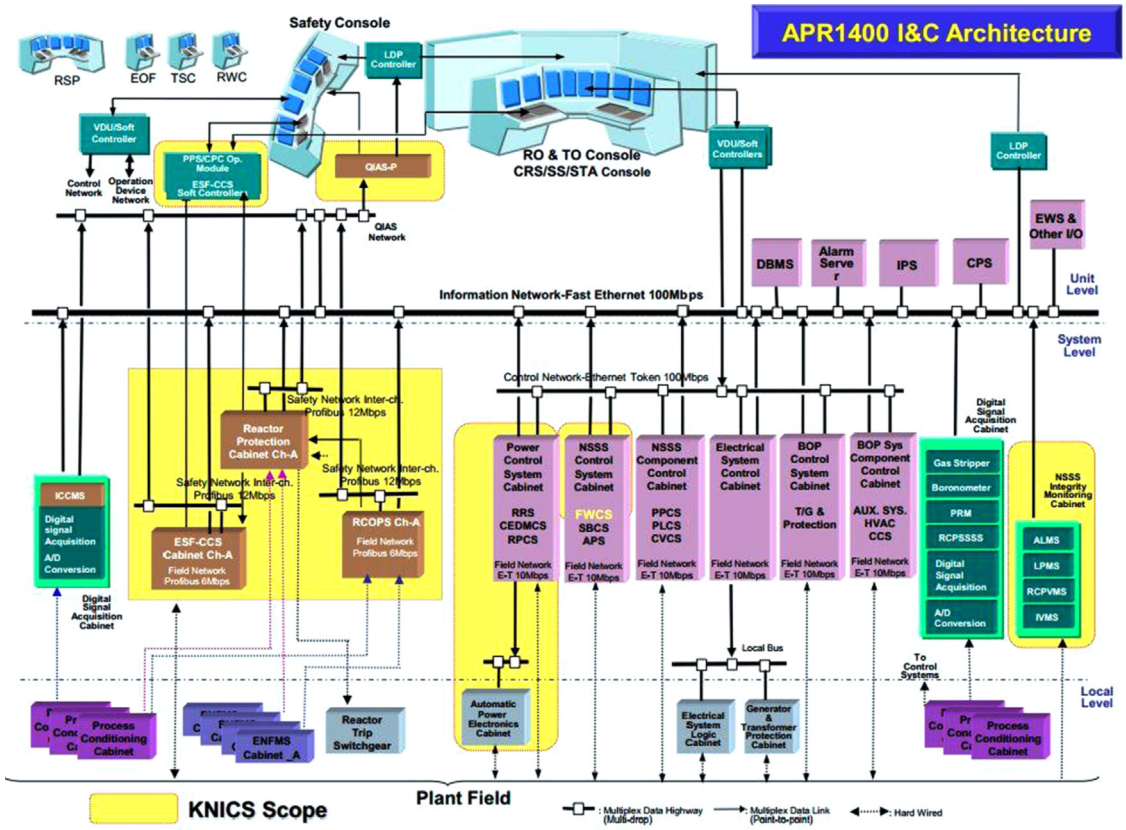


Fig. 1. APR-1400 MMIS Architecture [2].

evaluated [5]. However, a plant safety network should be analyzed in a different manner from that used to analyze a commercial network system because a plant safety network is based on a state-based communication system. Commercial network systems use a collision-based protocol, which introduces randomness into the network system. Such randomness is avoided in the design of safety network systems for NPPs. A state-based communication system is a system that communicates a fixed set of data at regular intervals. Such a system exhibits more predictable performance outside of standard operating conditions compared with commercial network systems at the cost of a less efficient use of communication bandwidth [6]. In this study, a framework for assessing the reliability of a safety network system based on the network communication protocol between GCs and LCs in the ESF-CCS in addition to 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 is developed. The hazardous states are identified by considering the Profibus-Decentralized Periphery (Profibus-DP) protocol operation, and a quantification scheme for various failure causes, including hardware failure, software failure and failure caused by the bit error in a token or data frame, for the identified hazardous states are discussed. A fault-tree model is developed based on the identified hazardous states considering the redundant structures of the GCs, LCs and network medium in the ESF-CCS, and the risk effects of network failures in the GCs and LCs on ESF-CCS signal failures are analyzed by conducting a sensitivity study based on the specified range of the periodic inspection periods of network modules and the baseline probability of software failure. This study is expected to provide insight into the identification of the hazardous states of network failure in a digital I&C system and the quantification of the risk effects of network failure on the transmission of safety-critical information in NPPs.

2. Target system

2.1. Engineered safety feature-component control system

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 engineered safety feature (ESF) initiation signals are generated by the plant protection system (PPS) and the radiation monitoring system (RMS) and are transmitted to the ESF-CCS, automatic manipulation 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 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, as shown in Fig. 2 [7]. The HR-SDN system uses the Profibus-DP protocol, which is based on send data with no acknowledge (SDN) communication; this protocol is a standard fieldbus protocol that is extensively applied in other industry fields [8]. Other network system implemented in ESF-CCS, such as ESF-CCS inter-division network (EIDN) and ESF-CCS division status network (EDSN), is used for the transmission of safety-related data, such as test results for voting logic conducted by GCs and LCs during manual testing of the system [3].

2.2. Profibus-DP protocol

To identify the potential hazardous states that might cause a system to enter an unsafe state, the operational characteristics of the Profibus-DP protocol must be considered. Two types of stations are defined in the Profibus-DP protocol: master stations and slave

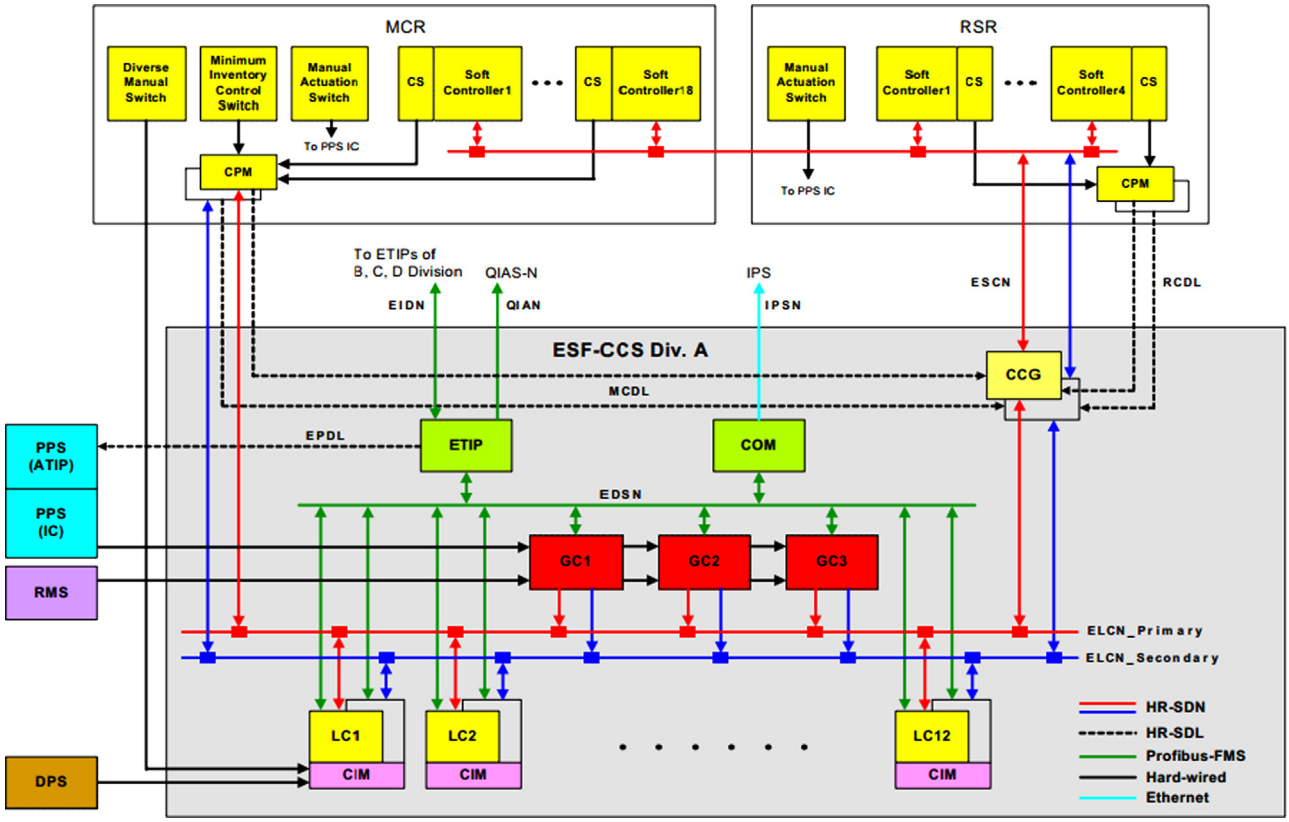


Fig. 2. ESF-CCS configuration (single division) [7].

stations [9]. The master station initiates the message cycle, whereas the slave station sends the acknowledgment or response frame. All stations in the target system can be regarded as master stations because the network communication between the GCs and LCs is based on a HR-SDN, which operates via peer-to-peer communication.

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 [10]. The IEEE has established the IEEE 802.4 standard, which specifies the services and a standard for local area networks (LANs) that use explicit token passing schemes to control access on a bus topology network [11]. In the token bus protocol, each station is assigned a location in an ordered sequence, with the last station in the sequence being followed by the first station. The logical topology of the token bus protocol follows a logical ring of active stations via the token passing process, whereas the physical topology follows a bus topology. Because each node only knows the address of its neighbor in the ring, a special protocol is needed to notify the other nodes of connections to or disconnections from the ring. A token bus network employs a small frame, which is known as a token frame, to grant individual stations exclusive access to the network transmission medium. When a station acquires control of the token frame, it becomes the temporary master of the stations in the ring of the network, and that station is allowed to transmit one or more data frames, depending on the token holding time, which is the time limit imposed by the network. When the station has finished using the token to transmit data, or the time limit has expired, it relinquishes control of the token, and the token is then passed through subsequent stations in the logical topological sequence until the lowest-addressed station acquires the token and passes the token to the active station with the highest address.

3. Proposed framework

Based on the general operational characteristics of the Profibus-DP protocol, the hazard states and the corresponding causes of failure for network communication between GCs and LCs can be identified. In this study, faults or errors of GCs and LCs are not considered; however, the failure of GCs and LCs, which can terminate the controllers' abilities to perform their functions, are considered when assessing the reliability of the target network communication system and the risk effects of network failure between GCs and LCs on ESF-CCS signal failure [12]. In other words, the error recovery process of the general token bus protocol, including the recovery process by medium access control (MAC), such as in response to lost or multiple tokens, a token passing failure, a deaf station or stations with duplicate addresses, was not considered because the coverage of these error recovery operations for network failure in ESF-CCS has not yet been investigated.

3.1. Identification of hazardous states 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 [13]. 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 [14]. Isolating errors are errors that can be isolated to a given fault domain, namely, a station, its upstream neighbor, and the wire

between them. Isolating errors include line errors, burst errors, internal errors, and abort errors. Non-isolating errors include lost frames, congestion, token errors, and frequency errors. In this study, the isolating errors were treated as the main failure causes in the Profibus-DP protocol; thus, the causes of these errors were categorized into hardware failure, software failure and failure caused by medium-related bit errors.

The general specifications of major operation process of Profibus-DP protocol are provided in the following sections, and the corresponding hazardous states and the failure causes are discussed. Table 1 lists the identified hazardous states and failure causes of the target network communication system.

3.1.1. Token reception

To send a data frame, a station must first receive a token frame from its upstream station. A station receives a token frame addressed to itself from a previous registered station. This process is related to the function of MAC: the failure of physical layer hardware can cause the failure of the token reception process. A software malfunction or MAC interruption can also cause a token reception failure. Because the token frame must be delivered to the station with the correct address from the previous registered station, a station can receive an erroneous token frame such as one that contains bit errors caused by noise or interference in the medium.

3.1.2. Data transmission

When a station receives a token frame, a service application block in the network module passes the token frame to the controller, which accepts the service request and attempts to transmit the data to the next station. In this case, the message dispatching functions are performed by the software; thus, a software interruption can cause a data transmission failure. Hardware failure in the physical layer of the network module should also be considered as a possible cause of data transmission failure.

3.1.3. Data reception

If the frame's destination address field matches the individual address, relevant group addresses, and active functional address of the designated station, then the data frame is copied after it is transmitted to that station and is subsequently indicated to the appropriate sublayer of the station. In this stage of operation, either hardware failure or software failure can result in a failure of data reception by the station. Data frame corruption caused by bit errors due to the introduction of noise in the transmission medium can also cause an incorrect data frame to be received, thus resulting in failure upon the reception of the data frame.

3.1.4. Token passing

When the data frame has been successfully delivered to the next station, the station then passes the token frame to the next token destination station and completes its message cycle. Similar to the case of data transmission, these functions are performed by the software, a service application block passes the token frame to its controller and the controller attempts to send the token frame to the next station. During this stage of operation, either hardware or software failure in the network module can cause the failure of a token passing operation.

3.2. Quantification of network failure probability

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. Therefore, either failure of the hardware components in the physical layer of the network module or failure of the software to function may cause network protocol failure, thereby resulting in a failure of token or data frame reception. In addition, electromagnetic interference or other environmental interference in the medium may cause bit errors or faults in a token or data frame and result in such a failure. To estimate the risk effects of network communication failure between GCs and LCs on ESF-CCS signal failure in a certain ESF initiation condition, a quantification scheme for each identified cause of failure was developed.

3.2.1. Hardware failure

The HR-SDN system is adopted for the network communication between GCs and LCs. This system is based on a safety-grade programmable logic controller (PLC) [2]. A PLC consists of various modules, including an input module, a processor module, an output module and network modules [15]. Based on PLC module data, the failure rates of the hardware components, with the exception of the network modules, were estimated based on the number of modules in each type of controller, as shown in Table 2 [16].

To estimate the failure rate of a network module, its sub-level hardware components, including the transmitter, the receiver, and other hardware modules, must be considered. In this study, the failure rates for various hardware components specified in the block diagram of the Profibus controller, including those for the

Table 1
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 network 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

Table 2
Failure rate of various modules in a single GC and LC [16,17].

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

Table 3
Failure rates for sub-level hardware components in a network module [19,20].

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

microprocessor, the interrupt controller, the serial interface, the application specific integrated circuit (ASIC), and the random access memory (RAM), were considered [18]. In this study, the failure probability for each hardware component was determined based on a reliability model for a digital feedwater control system [19]. Regarding the transmitter and receiver in the serial interface, the average failure rate for the photonic component was estimated based on the reliability data of photonic components and their subsystems [20] (Table 3).

To estimate the probability of hardware failure, the mean unavailability of the components of a network module must be considered. Consider the case of a general electric component that undergoes periodic inspection at specified intervals. The mean unavailability (Q_{ave}), or the time-dependent probability for a random failure, of a component with a constant failure rate of λ_0 can be calculated as one-half of the product of the failure rate (λ_0) and the periodic test interval (T) [21]:

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

In this study, two periodic test intervals for the hardware components in the network modules of the GCs and LCs were considered. The components in the network modules were assumed to be manually tested once per month and to undergo automatic periodic testing by the self-diagnostic function implemented in the PLC. General PLC operations include a self-diagnostic process or the PLC scan process, which enables internal diagnostics and communication task tests to be performed by the central processing unit (CPU) [22]. In general, the PLC scan is dependent on the complexity of the software program implemented in the PLC and the processing capability of the processor in the PLC. Generally, the PLC scan time ranges from a few milliseconds to one-hundred milliseconds. In this study, the interval of the automatic tests performed by the PLC self-diagnostics for the network module hardware components was assumed to be 50 ms. Because the functions of the GCs and LCs are based on repetitive network communication with fixed sets of transmitted data, all design-intended functions of the GCs and LCs were assumed to be tested in every PLC self-diagnostic cycle; thus, the coverage of the automatic test was assumed to be unity.

3.2.2. Software failure

Because software, unlike hardware, does not fail, break, or wear out over time, equivalent accelerated stress testing cannot be performed on software [5]. In principle, software takes inputs from other systems and produces outputs that are used either by humans or by other software and hardware. A previous study has suggested a qualitative approach that considers the complexity of the application function and the level of the verification and validation (V&V) process required for application software in a NPP [23]. In the proposed quantification method, indirect evidence is applied to estimate the failure probabilities of application software modules using the metrics of complexity and V&V level, for which the safety integrity level (SIL) is used as an estimator of the V&V process, as shown in Table 4. A value of 0 for the V&V level denotes a very simple or non-existent V&V process that does not fulfill any SIL class requirements, and the complexity of the system is classified as high, medium or low.

Because the GCs and LCs in the ESF-CCS also undergo a thorough V&V process for implementation in an NPP, the failure probability of the software implemented in the GCs and LCs can be similarly treated using this approach. With regard to the SIL class, the frequency of error occurrence in the GC and LC software can be considered to be infrequent, and the consequence of software failure can be considered to be critical because the software performs the function of transmitting safety-critical information. The software implemented in the GCs and LCs in the ESF-CCS exhibits low complexity in terms of software complexity because it is focused on the activation of safety-critical functions in NPPs [25]. Therefore, the sensitivity study in this study was conducted based on the assumption that the software failure probability ranges from 1.0E−04 to 1.0E−05, as reported in Tables 4 and 5.

3.2.3. Failure caused by medium-related bit errors

Safety-critical instrumentation generally falls into one of two operation modes which is continuous and low demand mode [26]. The safety-critical I&C system in NPP is operated as low demand mode since its safe operation is called upon at the time point of demand when NPP is at abnormal state. Therefore, the probability of the introduction of error in the transmitted data in ESF actuation condition can be treated as the probability of failure on demand (PFD). In addition, a single bit error in a token frame or data frame that is transmitted between GCs and LCs in the ESF-CCS was assumed to have a critical effect on the network communication, thus resulting in on-demand failure of network communication.

The Profibus-DP protocol uses coaxial cable or broadband as a transmission medium. When data are transmitted over a data link through coaxial cable, errors may be introduced into the network module as a result of noise or interference caused by external factors in the transmission medium. If errors are introduced into a token or data frame, then the integrity of the system, including the network module, may be compromised. In terms of the probability of the

Table 4
Baseline failure probability estimates for application software modules [23].

SIL	Complexity of the software		
	High	Medium	Low
0	1.0E−01	1.0E−02	1.0E−03
1	1.0E−02	1.0E−03	1.0E−04
2	1.0E−03	1.0E−04	1.0E−05
3	1.0E−04	1.0E−05	1.0E−06
4	1.0E−05	1.0E−06	1.0E−07

introduction of error into the system, the bit error rate (BER) is a key parameter that is used to assess systems that transmit digital data between locations. Generally, systems for which the BER is applicable include fiber-optic data systems and other systems, such as Profibus-DP network systems, that transmit data over a transmission medium in which noise and interference may cause degradation of the digital signal. In the case of network communication in a communications system, the BER on the receiver side may be affected by transmission channel noise, interference, and distortion, among other factors; it is defined as the ratio of the number of bit errors in the transmitted bits to the total number of transmitted bits [27]. In the Profibus network, physical layer implementation is generally specified for three types, and each type exhibits particular signaling rates and transmission characteristics; however, the BER of each physical layer implementation is generally on the order of 1.0E−08 [28]. In this study, the estimated expected number of erroneous bits in each frame was treated as the probability of token frame or data frame corruption caused by bit errors introduced by the bus medium, which depends on the length of the token frames and the data frames in the Profibus-DP protocol, as shown in Fig. 3 [29].

3.3. Fault-tree analysis of network communication in GCs and LCs

In the previous study, the feasibility of applying a fault-tree analysis to the reliability assessment of safety-critical digital systems was demonstrated using a case study for the digital reactor protection system of NPPs [30]. The fault-tree analysis of safety-critical digital systems provides various advantages in the risk-informed design of the digital system, including the reliability analysis of a multi-channel digital system and the identification of the critical factors in the digital system safety based on the sensitivity study. Because ESF-CCS has four redundant channels, where each channel is equipped with three redundant GCs and doubly redundant LCs, the fault-tree analysis of ESF-CCS signal failure in a certain ESF initiation condition was developed for the case study.

3.3.1. Functional allocation of the ESF-CCS divisions

The ESF-CCS consists of four redundant divisions (i.e., A–D). In each division, there are three redundant GCs (e.g., GC A1, A2, and A3), which perform the function of selective two-out-of-four coincidence logic for the four safety component actuation signals from each PPS channel, and 12 LCs, which are functionally allocated to various field components such as pumps and valves.

Table 5
IEEE standard for software integrity level [24].

Consequence	Frequency of error occurrence in the software			
	Reasonable	Probable	Occasional	Infrequent
Catastrophic	4	4	4 or 3	3
Critical	4	4 or 3	3	2 or 1
Marginal	3	3 or 2	2 or 1	1
Negligible	2	2 or 1	1	1

Each loop controller has a doubly redundant structure, consisting of a main LC and a hot standby backup LC (e.g., LC A1a and LC A1b); the controller performs the function of two-out-of-three component control auctioneering of the signals, which are received by each of the three GCs. When the malfunction of a main loop controller is detected, the hot standby backup LC assumes the task of the main LC to initiate the safety signal being transmitted from the corresponding GCs. The network medium also has a doubly redundant structure (e.g., Network A1 and A2), in which each network medium transmits a data frame from the three GCs to the corresponding LC for a specific safety component actuation signal. Fig. 4 illustrates the conceptual layout of the ESF-CCS [4].

In terms of the functional allocation of the LCs in the ESF-CCS, the system is composed of approximately 300 components related to various safety actuation signals provided by the ESF-CCS, including the safety injection actuation signal (SIAS) and the containment spray actuation signal (CSAS). All safety injection components are functionally allocated in the four safety-related divisions; approximately 110 components are equally divided among the four divisions. In each division of the ESF-CCS, the safety functions are also functionally allocated in each LC.

3.3.2. Case study

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. [4] 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, as shown in Table 6.

Based on Table 1, which summarizes the potential hazardous states and the corresponding causes of failure that may cause a failure of network communication in the Profibus protocol, the fault-tree model of network failure in the GCs and LCs is modeled using the Advanced Information Management System for Probabilistic Safety Assessment (AIMS-PSA), which is an integrated safety assessment software package developed at KAERI. The logic of the model is illustrated in Fig. 5. To analyze the risk effects of network communication failure on ESF-CCS signal failure, the top-event cut sets were generated based on the developed fault-tree model.

In terms of network communication failure between 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 GCs and LCs can also lead to a failure to provide input to the corresponding LCs. As shown in Fig. 5, 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),

a

Header	SD (=DCH)	DA	SA	ED (=16H)
Length	1 byte	1 byte	1 byte	1 byte

b

Header	SD(=A2H)	DA	SA	FC	DU	FCS	ED (=16H)
Length	1 byte	1 byte	1 byte	1 byte	8 bytes	1 byte	1 byte

Fig. 3. Profibus-DP protocol frame structure: (a) token frame format and (b) data frame format with fixed lengths of the data units.

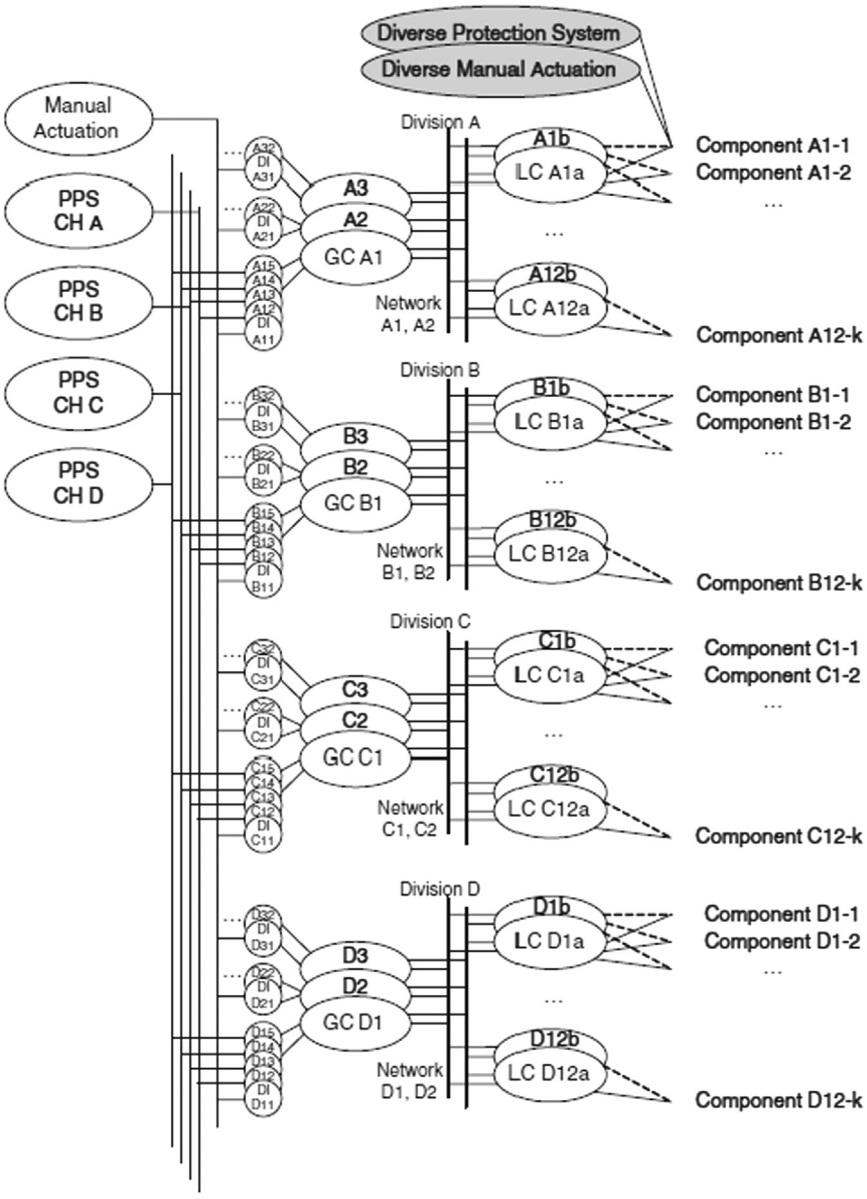


Fig. 4. Conceptual layout and signal flow of the ESF-CCS [4].

Table 6
Example of corresponding field components in allocated LCs in the CSAS condition.

ESF-CCS signal	Related components	Allocated LC
CSAS-A	PP01A	LC A3
	CSV35	LC C3
CSAS-B	PP01B	LC B3
	CSV36	LC D3

which is both physically and electrically separated from PPS and provides partial back-up means to the PPS in the case of automatic signal generation failure by the ESF-CCS, is also considered. The failure probability of the human operator for manual actuation of ESF signal generation via DPS was assumed as 0.05 and that of the field component via component interface module (CIM) is assumed as 0.1 based on the conventional human error probability (HEP) method [4].

As previously mentioned, a failure of network communication between the GCs and LCs may cause a failure to provide input to the corresponding LCs, including both the main LC (e.g., LC A3A) and the hot standby backup LC (e.g., LC A3B). When evaluating the possibility of network failure in the LC, both the failure of the network interface module in the LC and the failure of the network communication protocol should be considered, as shown in Fig. 6. Moreover, to model the failure of multiple identical components in the network interface, transmitter and receiver module as a result of shared causes, the common-cause failure of the network modules in the main and backup LCs can be considered by assuming the beta factor to be one tenth, based on the beta factor model [31]. Because the LC receives the data frame containing the safety component actuation signals from three GCs, the possibility of software failure of the LC and failure related to network-medium-related bit errors in the receipt of data frames from each GC must also be considered.

To account for network failure in a GC, both the failure of an independent hardware component (e.g., power supply, processor, or digital input) of the GC and the network communication failure of the GC are considered. Because each GC receives a token frame to send data to the allocated LCs and then passes the token frame

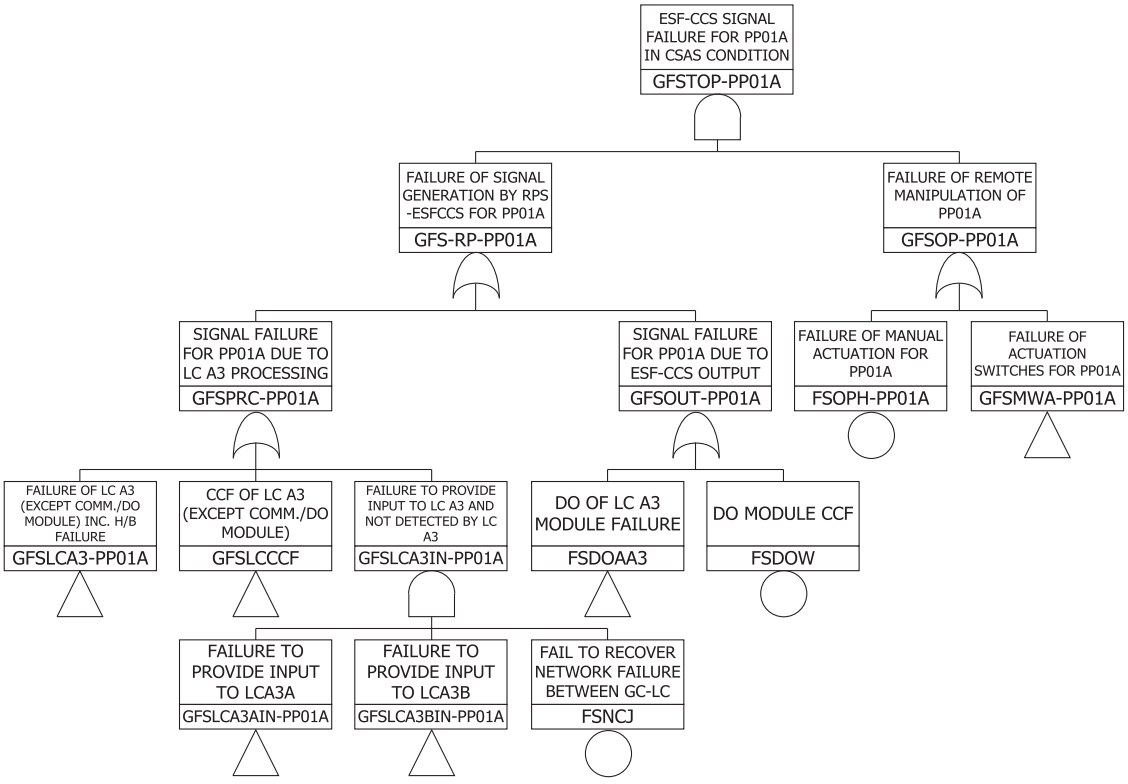


Fig. 5. Top logic of the developed fault-tree model of the ESF-CCS (CSAS-a signal failure for the field component PP01A; GFSTOP-PP01A).

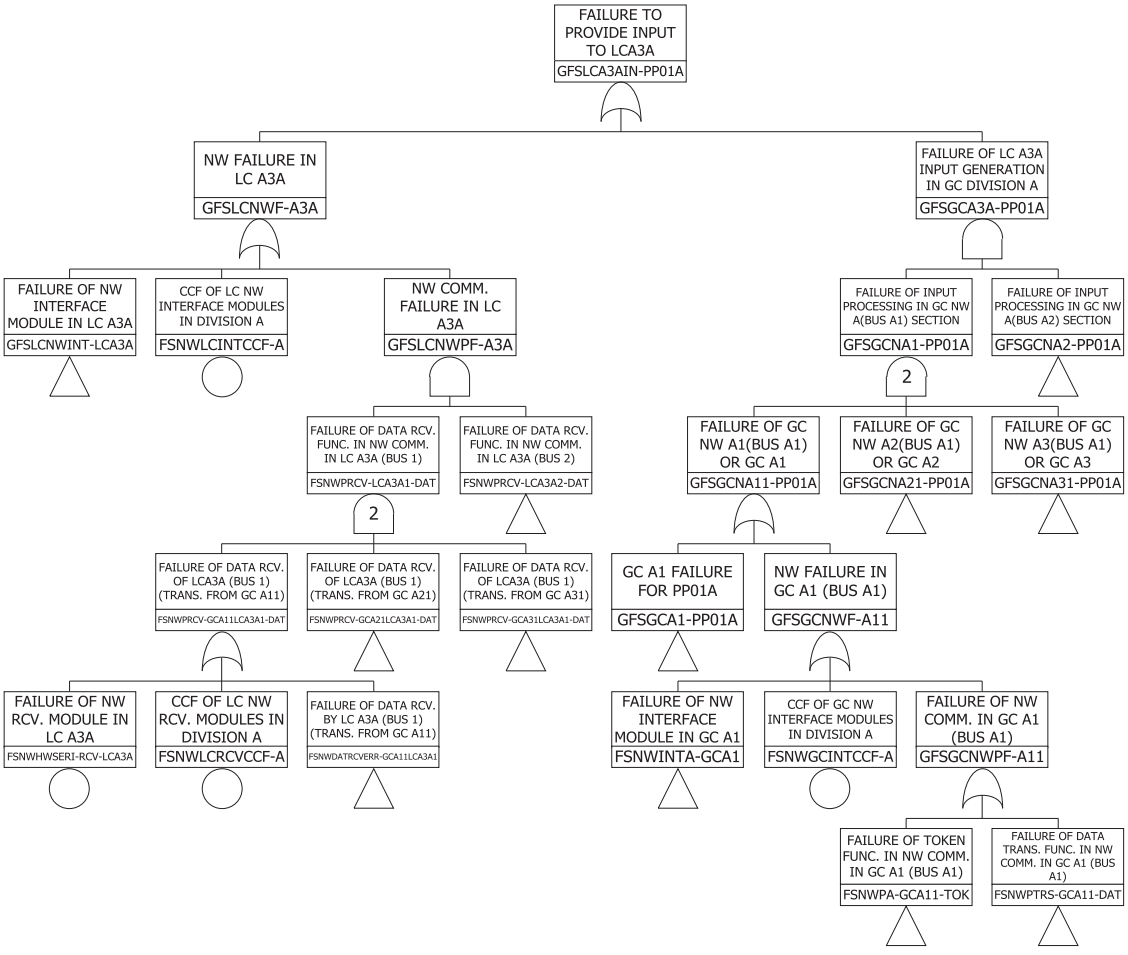


Fig. 6. Logic of the developed fault-tree model of the ESF-CCS (failure to provide input to the main LC, LC A3A, from the CSAS-A signal from the three GCs).

to the next designated station, the possibility of software failure for each identified Profibus operation is modeled in the fault-tree model, and token frame corruption caused by network-medium-related bit errors is also considered.

To estimate the risk effects of network communication failure on ESF-CCS signal-generation failure, the probabilities of hardware failure, software failure, and token data frame corruption are modeled based on the quantification scheme for each failure cause. In this manner, the top-event cut sets were generated, and the risk effects of network communication failure between 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

Based on the quantification scheme for each failure cause, 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 7.

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 GCs and LCs. As shown in Fig. 7, 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 (CCF) 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. 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. The quantification results of each case study are summarized in Table 8.

4.2. Risk effect of network communication 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. As shown in Table 9, the results indicate that overall network communication failure – which was calculated as the sum of the failure probabilities of the hardware components, including the interface, receiver and transmitter modules; the probability of failure of software operation in the network module; and the probability of frame corruption caused by noise 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.

The quantification results also reveal the important failure causes that contribute to network communication failure in the ESF-CCS. For cases 1 and 2, in which manual periodic inspection is assumed, the hardware failure of the network modules is regarded as an important failure cause contributing to overall network communication failure in the ESF-CCS. For cases 3 and 4, in which the automatic periodic testing performed by the PLC self-diagnostics is assumed, the failure of the software functions implemented in the network module is a dominant factor and contributes to overall network communication failure in the ESF-CCS.

5. Discussion

Note that the ESF-CCS is a newly developed system, whose detailed design and component configuration have not yet been fixed; thus, the results discussed in this study may not be comparable with the results of other studies of the ESF-CCS. However, the assumptions and fault-tree model used in the case study can be employed as a basis for the development of a fault-tree model based on a detailed ESF-CCS design that includes the detailed periodic inspection intervals for both automatic and manual tests of the network modules in the ESF-CCS and the detailed functional allocation of each division and LC for corresponding field components under various ESF signal actuation conditions.

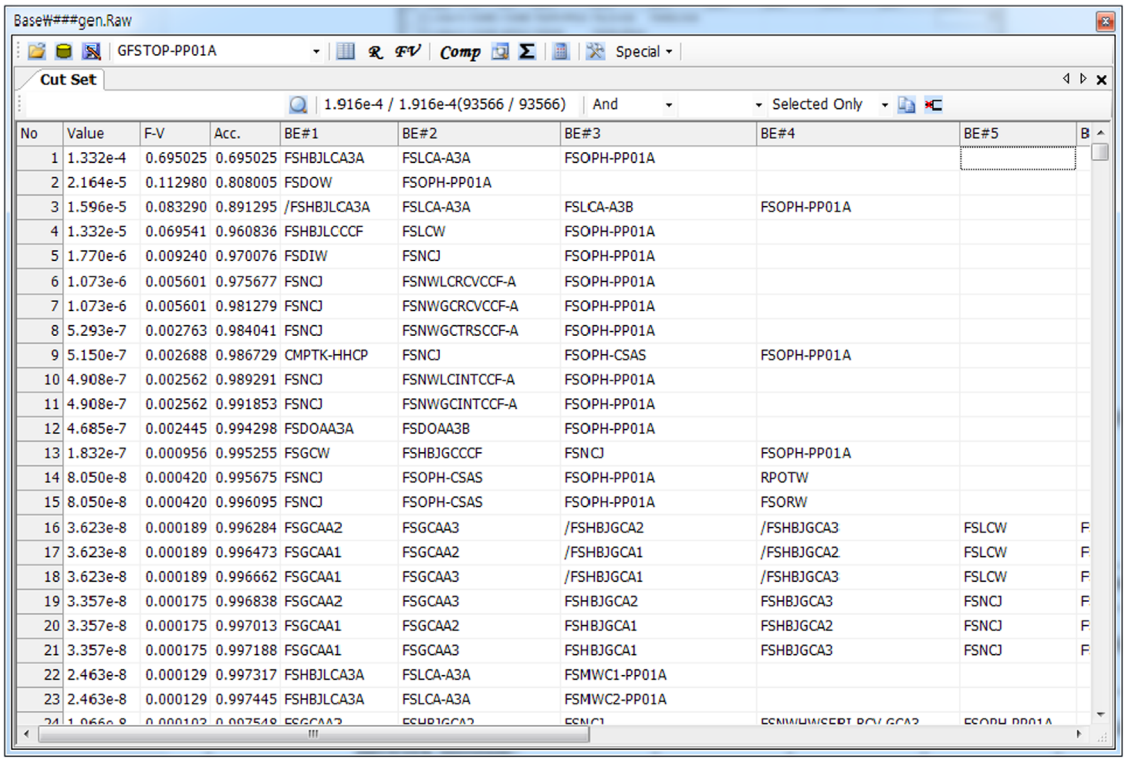
In this study, the risk effects of network failure between GCs and LCs in the ESF-CCS on ESF-CCS signal failure for a single field component under certain safety component actuation conditions were analyzed. However, the risk effects of network failure between GCs and LCs under various ESF signal conditions on the core damage frequency (CDF) of the NPP must be analyzed to address the effect of using a digitally based ESF-CCS on plant risk.

When expanding the component-level reliability model developed in this study to the system-level reliability model, CCFs should be considered carefully in calculating the unavailability of the multi-channel system since the ratio of unavailability from the combination of CCF and independent failures of the modules to the system unavailability becomes larger as the system configuration is complicated with multiple number of channels [32]. Since ESF-CCS is consisted of four divisions in which multiple GCs and LCs are located, modeling the CCF of the network components in multiple divisions must be investigated. Furthermore, the risk effects of network failure in the ESF-CCS on the CDF can be estimated in a more detailed manner by analyzing the failure modes and failure causes, in a sub-component level by means of failure mode and effects analysis (FMEA) and the fault detection coverage (FDC) of the fault tolerance techniques (FTTs) for the associated hazardous states after the detailed configuration of ESF-CCS is decided [33]. Based on the module-specific FMEA, the unavailability of the hardware components can be optimistically estimated by considering the estimated FDC of the FTTs and test interval for both manual testing and self-diagnostics.

In addition, the relationship among the human action failures must be investigated to consider multiple human error condition since ESF-CCS provides multiple manual actuation to assure the diversity of the system. Since the conventional HEP method cannot accommodate the multiple conditions in a fault tree, condition-

Table 7
Summary of the values adopted in the four case studies.

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 h	730 h	50 ms	50 ms



No	Value	F-V	Acc.	BE#1	BE#2	BE#3	BE#4	BE#5	B
1	1.332e-4	0.695025	0.695025	FSHBJLCA3A	FSLCA-A3A	FSOPH-PP01A			
2	2.164e-5	0.112980	0.808005	FSDOW	FSOPH-PP01A				
3	1.596e-5	0.083290	0.891295	/FSHBJLCA3A	FSLCA-A3A	FSLCA-A3B	FSOPH-PP01A		
4	1.332e-5	0.069541	0.960836	FSHBJLCCCF	FSLCW	FSOPH-PP01A			
5	1.770e-6	0.009240	0.970076	FSDIW	FSNCJ	FSOPH-PP01A			
6	1.073e-6	0.005601	0.975677	FSNCJ	FSNWLCRCVCCF-A	FSOPH-PP01A			
7	1.073e-6	0.005601	0.981279	FSNCJ	FSNWGCRCVCCF-A	FSOPH-PP01A			
8	5.293e-7	0.002763	0.984041	FSNCJ	FSNWGCTRSCCF-A	FSOPH-PP01A			
9	5.150e-7	0.002688	0.986729	CMPTK-HHCP	FSNCJ	FSOPH-CSAS	FSOPH-PP01A		
10	4.908e-7	0.002562	0.989291	FSNCJ	FSNWLCINTCCF-A	FSOPH-PP01A			
11	4.908e-7	0.002562	0.991853	FSNCJ	FSNWGCINTCCF-A	FSOPH-PP01A			
12	4.685e-7	0.002445	0.994298	FSDOAA3A	FSDOAA3B	FSOPH-PP01A			
13	1.832e-7	0.000956	0.995255	FSGCW	FSHBJGCCCF	FSNCJ	FSOPH-PP01A		
14	8.050e-8	0.000420	0.995675	FSNCJ	FSOPH-CSAS	FSOPH-PP01A	RPOTW		
15	8.050e-8	0.000420	0.996095	FSNCJ	FSOPH-CSAS	FSOPH-PP01A	FSORW		
16	3.623e-8	0.000189	0.996284	FSGCAA2	FSGCAA3	/FSHBJGCA2	/FSHBJGCA3	FSLCW	F
17	3.623e-8	0.000189	0.996473	FSGCAA1	FSGCAA2	/FSHBJGCA1	/FSHBJGCA2	FSLCW	F
18	3.623e-8	0.000189	0.996662	FSGCAA1	FSGCAA3	/FSHBJGCA1	/FSHBJGCA3	FSLCW	F
19	3.357e-8	0.000175	0.996838	FSGCAA2	FSGCAA3	FSHBJGCA2	FSHBJGCA3	FSNCJ	F
20	3.357e-8	0.000175	0.997013	FSGCAA1	FSGCAA2	FSHBJGCA1	FSHBJGCA2	FSNCJ	F
21	3.357e-8	0.000175	0.997188	FSGCAA1	FSGCAA3	FSHBJGCA1	FSHBJGCA3	FSNCJ	F
22	2.463e-8	0.000129	0.997317	FSHBJLCA3A	FSLCA-A3A	FSMWC1-PP01A			
23	2.463e-8	0.000129	0.997445	FSHBJLCA3A	FSLCA-A3A	FSMWC2-PP01A			

Fig. 7. Dominant top-event cut sets of the fault tree (CSAS-a signal failure for the field component PP01A; GFSTOP-PP01A) for case 1.

Table 8
Summary of quantification results for each failure cause in the case studies.

Description	Case 1	Case 2	Case 3	Case 4
Failure of hardware components in the network module	3.58E−06	3.58E−06	6.96E−14	6.96E−14
Failure of software implemented in the network module	2.88E−08	2.81E−09	1.31E−08	1.24E−09
Failure caused by token/data frame corruption	1.04E−16	1.02E−16	5.29E−17	5.07E−17
ESF-CCS signal failure for PP01A in the CSAS condition	1.92E−04	1.92E−04	1.88E−04	1.88E−04

Table 9
Risk effects of network failure on ESF-CCS signal failure in the case studies.

Description	Case 1	Case 2	Case 3	Case 4
Overall network communication failure on ESF-CCS signal failure for PP01A in the CSAS condition	1.88 (%)	1.87 (%)	7.01E−03 (%)	6.63E−04 (%)

based human reliability assessment method can be applied to include a complex relationship among the automated safety signal generation and the human operator's manual actuation, avoiding the optimistic estimation of HEP of the human action failure [34].

6. Conclusion

The ESF-CCS, which employs a network communication system for the transmission of safety-critical information from the GCs to the LCs, was developed to effectively accommodate a vast number of field controllers. However, the application of the developed ESF-CCS in NPPs has faced challenges regarding the regulatory requirements of safety-related digital systems because the risk effects of network communication failure on the overall plant risk have not yet been completely quantified. Therefore, a framework for identifying the potential hazardous states of network communication in the ESF-CCS and quantifying the corresponding causes was proposed, and a fault-tree model for network communication failure was developed to estimate the risk effects of network failure between 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. The dominant failure cause contributing to the overall likelihood of network communication failure in the ESF-CCS was identified based on these results. 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 GCs and LCs under other ESF initiation conditions.

This study is expected to provide insight into the development of the fault-tree model for the network failure in digital I&C system and into the quantification of the risk effect of network failure for safety-critical information transmission in NPPs. As an extension of this study, future studies will investigate extending the fault-tree model developed in this study to the network communication between GCs and LCs under various ESF signal conditions after a detailed ESF-CCS design is prepared.

Acknowledgment

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. DC, USA: National Academy Press; 1997.
[2] Lee, Dong Young, et al. Development experiences of a digital safety system in Korea. In: Proceedings of the IAEA technical meeting on the impact of Digital I&C Technology on the operation and licensing of NPP. Beijing, China, November; 2008.
[3] Kim Dong Hoon, et al. Development of design methodology for communication network in nuclear power plants. Daejeon, Republic of Korea: Korea Atomic Energy Research Institute; 1996.
[4] Kang Hyun Gook, Jang Seung-Cheol. A quantitative study on risk issues in safety feature control system design in digitalized nuclear power plant. J Nucl Sci Technol 2008;4(8):850–8.
[5] Leveson G Nancy. Safeware: system safety and computers. Reading, MA: Addison-Wesley Professional; 1995.
[6] Preckshot G George. Data communications. DC, USA: U.S. Nuclear Regulatory Commission; 1993.
[7] Kim, Seong Tae, et al. New design of engineered safety features-component control system to improve performance and reliability. In: Proceedings of the 15th pacific basin nuclear conference, Sydney, Australia, October 15–20; 2006.
[8] Kim Young Jin, et al. Design support for ESF-CCS. Daejeon, Republic of Korea: Korea Atomic Energy Research Institute; 2008.
[9] Tovar Eduardo, Francisco Vasques. Real-time fieldbus communications using Profibus networks. IEEE Trans Ind Electron 1999;46(6):1241–51.
[10] Willig Andreas, Wolisz Adam. Ring stability of the PROFIBUS token-passing protocol over error-prone links. IEEE Trans Ind Electron 2001;48(5):1025–33.
[11] IEEE, IEEE Standards for Local Area Networks: Token-Passing Bus Access Method and Physical Layer Specification, IEEE, New York, USA; 1985.
[12] Kim Man Cheol, Carol S Smidts. Three suggestions on the definition of terms for the safety and reliability analysis of digital systems. Reliab Eng Syst Saf 2015;135:81–91.
[13] Elahi Ata. Network communications technology. MA: Cengage Learning; 2001.
[14] Haugdahl J Scott. Network analysis and troubleshooting. Reading, MA: Addison-Wesley Professional; 2000.
[15] Koo Seo Ryong, Poong Hyun Seong. Software design specification and analysis technique (SDSAT) for the development of safety-critical systems based on a programmable logic controller (PLC). Reliab Eng Syst Saf 2006;91(6):648–64.
[16] Hur, Seop, et al. Reliability analysis and component functional allocations for the ESF multi-loop controller design. In: Proceedings of the third international conference on reliability, safety and hazard (ICRESH-05), Mumbai, India, December 1–3; 2005.
[17] Lee Dong-Young, Choi Jong-Gyun, Lyou Joon. A safety assessment methodology for a digital reactor protection system. Int J Control Autom Syst 2006;4(1):105–12.
[18] Siemens, SIMATIC NET ASPC 2/Hardware User Description. Siemens AG, Germany; 1997.
[19] Chu, TL, et al. Modeling a Digital feedwater control system using traditional probabilistic risk assessment methods NUREG/CR-6997, US Nuclear Regulatory Commission; 2009.
[20] Quanterion Solutions Inc. Photonic Component and Subsystem Reliability Process Final Report, Penn State University Electro-Optics Center, PA, USA; 2008.
[21] Ohring Milton. Reliability and failure of electronic materials and devices. San Diego, CA: Academic Press; 1998.
[22] Maher, J Michael. Real-time control and communications. In: Proceedings of the 18th annual ESD/SMI International programmable controllers conference; 1989.
[23] Bäckström, Ola, et al. Quantification of reactor protection system software reliability based on indirect and direct evidence. Probabilistic safety assessment and management (PSAM 12), Honolulu, Hawaii, June 22–27; 2014.
[24] IEEE Computer Society. IEEE Standard for Software Verification and Validation, IEEE, New York, USA; 2005.
[25] Lee Dong Young, et al. Development of the digital reactor safety system. Daejeon, Republic of Korea: Korea Atomic Energy Research Institute; 2008.
[26] Brown Simon. Overview of IEC 61508. Design of electrical/electronic/programmable electronic safety-related systems. Comput Control Eng J 2000;11.1:6–12.
[27] Jeruchim C. Techniques for estimating the bit error rate in the simulation of digital communication systems. IEEE J Sel Areas Commun 1984;2.1:153–70.
[28] Irwin J David. The industrial electronics handbook. Boca Raton, FL: CRC Press; 1997.
[29] Acromag Incorporated. BusWorks 900 PB Series ProfiBus/RS485 Network I/O Modules Technical Reference, Introduction to ProfiBus DP, Acromag Incorporated, MI, USA; 2002.
[30] Kang Hyun Gook, Sung Tae yong. An analysis of safety-critical digital systems for risk-informed design. Reliab Eng Syst Saf 2002;78(3):307–14.
[31] Heising D Carolyn, Ching N Guey. A comparison of methods for calculating system unavailability due to common cause failures: the beta factor and multiple dependent failure fraction methods. Reliab Eng 1984;8(2):101–16.
[32] Kang Hyun Gook, Kim Hee Eun. Unavailability and spurious operation probability of k-out-of-n reactor protection systems in consideration of CCF. Ann Nucl Energy 2012;49:102–8.
[33] Lee Seung Jun, et al. Reliability assessment method for NPP digital I&C systems considering the effect of automatic periodic tests. Ann Nucl Energy 2010;37(11):1527–33.
[34] Kang Hyun Gook Jang Seung-Cheol. Application of condition-based HRA method for a manual actuation of the safety features in a nuclear power plant. Reliab Eng Syst Saf 2006;91(6):627–33.