A Quantitative Assessment Method for Trip Signal Generation Failures

Seung Ki Shin [a], Poong Hyun Seong [a*]
[a]*Department of Nuclear and Quantum Engineering, KAIST*
373-1, Guseong-dong, Yuseong-gu, Daejeon, Republic of Korea, 305-701
[*]*Corresponding author: phseong@kaist.ac.kr*

1. Introduction

Safety-critical systems such as nuclear power plant protection systems are introducing digital technologies in an effort to enhance safety [1, 2]. In order to analyze a process in which a certain accident occurs and where the protection systems cannot diagnose the plant status correctly, implying that the proper safety-critical signals will not be generated, it is necessary to consider the occurrence of the accident, the component failures of the instrumentation and control (I&C) systems concurrently, not separately. Hence, this paper proposes a quantitative analysis method to assess the entire process of the initial occurrence of an accident, the recognition of plant state changes and the final generation of safety-critical signals by automated protection systems using dynamic RGGG (Reliability Graph with General Gates) method [3].

2. Dynamic Dependencies between Accidents and I&C Devices

Considering the relationships between components of I&C systems, the reasons for a specific safety function failure can be expressed using a static fault tree [4]. However, when the top event is a failure of the reactor trip, the occurrence of an accident and the failure of the safety function must be considered concurrently. In addition, a static gate cannot represent the relationship between these two events, as the failure of a reactor trip depends on the sequence of events. For example, even when some of the instrumentation sensors fail, automated systems can recognize changes in the plant state if the sensors fail after an accident occurs, thus allowing the correct reactor trip signals to be generated. Therefore, a dynamic system analysis method should be utilized to model and analyze these relationships quantitatively.

2.1 Development of a dynamic recognition node

Conventional modeling methods cannot depict the recognition process of plant state changes by automated plant protection systems. This situation arises because automated systems cannot recognize plant state changes only in the event that automated systems or sources of information such as sensors fail before an accident occurs. In order for the systems to recognize plant state changes, the signals from information sources should be available when plant states change due to an accident. In order to describe the relationships between an accident and the sources of information, a novel dynamic node, the recognition node in Fig. 1, is developed and rules are proposed to determine a probability table for the node.

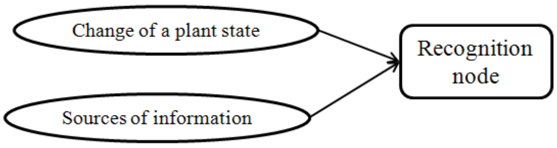

Fig. 1. A recognition node

Let the outputs of the node for a change in a plant state, the node for the sources of information, and the recognition node be I_x, I_y, and I_z, respectively. ($x, y, z \in 1, 2 \ldots n, \infty$) Each blank in the probability table for the recognition node that is defined by x, y, and z can then be filled in on the basis of the following rules and shown in Table I. P_k refers to the probability that a subject recognizing a plant state change fails in the kth interval.

i. If $z > x$, *0*
ii. If $z = x > y$, *0*
iii. If $z = x \le y$, $1 - \sum_{k=1}^{z-1} P_k$
iv. If $z > x$, *0*
v. If $z = \infty$, *1 – (sum of the other probabilities in the same row).*

Table I: Probability table for a recognition node

		Recognition				
Change of a plant state	Sources of information	I_1	I_2	I_3	...	I_∞
I_1	I_1	*1*	*0*	*0*	...	*0*
	I_2	*1*	*0*	*0*	...	*0*
	I_3	*1*	*0*	*0*	...	*0*
	...	...	...	...	...	...
	I_∞	*1*	*0*	*0*	...	*0*
I_2	I_1	*0*	*0*	*0*	...	*1*
	I_2	*0*	$1\text{-}P_1$	*0*	...	P_1
	I_3	*0*	$1\text{-}P_1$	*0*	...	P_1
	...	...	...	...	...	...
	I_∞	*0*	$1\text{-}P_1$	*0*	...	P_1
I_3	I_1	*0*	*0*	*0*	...	*1*
	I_2	*0*	*0*	*0*	...	*1*
	I_3	*0*	*0*	$1\text{-}(P_1+P_2)$	...	P_1+P_2
	...	...	...	...	...	...
	I_∞	*0*	*0*	$1\text{-}(P_1+P_2)$	...	P_1+P_2
...	...	...	...	...	...	...
I_∞	I_1	*0*	*0*	*0*	...	*1*
	I_2	*0*	*0*	*0*	...	*1*
	I_3	*0*	*0*	*0*	...	*1*
	...	...	...	...	...	...
	I_∞	*0*	*0*	*0*	...	*1*

3. A Quantitative Assessment Method for Trip Signal Generation Failures

A dynamic RGGG for the automated trip signal generation process is shown in Fig. 2. If an accident occurs, various plant states change, and each sensor detects the change in each plant state. Whether the automated systems can recognize each plant state change depends on the sequence of the accident, the sensor failure, and the automated system failure; hence, the dynamic recognition nodes proposed in section 2.1 are used in the RGGG.

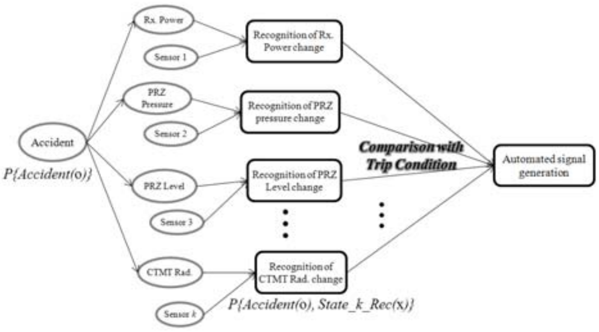
Rx. Power
Sensor 1
PRZ Pressure
Sensor 2
Accident
P{Accident(o)}
PRZ Level
Sensor 3
CTMT Rad.
Sensor k
Recognition of Rx. Power change
Recognition of PRZ pressure change
Recognition of PRZ Level change
Recognition of CTMT Rad. change
P{Accident(o), State_k_Rec(x)}
Comparison with Trip Condition
Automated signal generation

Fig. 2. A dynamic RGGG for automated protection systems

From each recognition node, a quantitative result is obtained; this is the probability that an accident will occur and that the automated system will not recognize each state change. This can be expressed as *P{Accident(*o*), State_k_Rec(*x*)}*. The conditional probabilities that the system will not recognize each state change given the occurrence of an accident can be obtained through the following equation.

$$P\{State\_k\_Rec(\mathrm{x}) \mid Accident(\mathrm{o})\}$$
$$= P\{Accident(\mathrm{o}),\ State\_k\_Rec(\mathrm{x})\}\ /\ P\{Accident(\mathrm{o})\}$$

If a system input parameter is associated with a reactor trip and it exceeds a set-point value, then the automated protection systems generate reactor trip signals. Therefore, when $\{State\_k \mid k = 1, 2, \ldots, i\}$ is associated with a reactor trip, the conditional probability, $P\{Automated\ Signals(\mathrm{x}) \mid Accident(\mathrm{o})\}$ can be calculated as follows:

$$P\{Automated\ Signals(\mathrm{x}) \mid Accident(\mathrm{o})\}$$
$$= \prod_{k=1}^{i} P\{State\_k\_Rec(\mathrm{x}) \mid Accident(\mathrm{o})\}$$

Finally, the probability that automated trip signals are not generated despite the fact that an accident occurs can be calculated as follows:

$$\mathrm{P}\{Accident(\mathrm{o}), Automated\ Signals(\mathrm{x})\}$$
$$= P\{Automated\ Signals(\mathrm{x}) \mid Accident(\mathrm{o})\} \times P\{Accident(\mathrm{o})\}$$

This result is smaller (more accurate) than the result estimated using the static methods.

4. Conclusions

As nuclear power plants become digitalized, in the case of accidents, automated protection systems generate safety-feature-actuation-signals to prevent the propagation of accidents. To assess whether or not the automated systems can generate the safety signals, a sequence of points in time in which an accident occurs and I&C devices fail should be considered. In this paper, the total process in which an accident occurs and in which the automated systems cannot recognize changes in various plant parameters due to failures of I&C devices is modeled with a dynamic RGGG method. Additionally, quantitative assessments are conducted. Using the dynamic RGGG method, the complex systems and the information flows can be modeled easily and intuitively. For a quantitative analysis, although the true value cannot be obtained from the dynamic RGGG owing to the discrete-time method, the steady state explosion problem arising from the Markov chain method is avoidable and a value very close to the true value can be estimated by increasing the number of intervals. Thus, the dynamic RGGG method has advantages when used for the analyses of complex systems such as nuclear power plants. The proposed analysis method can be applied to the assessments of the generation of safety signals as well as to various dynamic situations in safety-critical systems, such as nuclear power plants.

REFERENCES

[1] US Nuclear Regulatory Commission (USNRC), Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments, NUREG/CR-6901, Washington DC, 2006.

[2] P. H. Seong, et al., Reliability and Risk Issues in Large Scale Safety-critical Digital Control Systems, Springer, London, 2008.

[3] S. K. Shin, P. H. Seong, Review of Various Dynamic Modeling Methods and Development of an Intuitive Modeling Method for Dynamic Systems, Nuclear Engineering and Technology, Vol.40, p. 375, 2008.

[4] H. G. Kang, S. C. Jang, Application of Condition-based HRA Method for a Manual Actuation of the Safety Features in a Nuclear Power Plant, Reliability Engineering and System Safety, Vol.91, p.627, 2006.