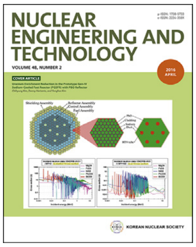
Available online at ScienceDirect

Nuclear Engineering and Technology

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



Original Article

Improvement of the Reliability Graph with General Gates to Analyze the Reliability of Dynamic Systems That Have Various Operation Modes

Seung Ki Shin [a], *Young Gyu No* [b], *and Poong Hyun Seong* [b,*]

[a] *Division of Research Reactor System Design, Korea Atomic Energy Research Institute,*
Daedeok-daero 989-11, Yuseong-gu, Daejeon 305-353, Republic of Korea
[b] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology,*
Daehak-ro 291, Yuseong-gu, Daejeon 305-338, Republic of Korea

ARTICLE INFO

Article history:
Received 25 June 2015
Received in revised form
4 September 2015
Accepted 25 November 2015
Available online 21 December 2015

Keywords:
Bayesian Networks
Dynamic Fault Tree
Probabilistic Risk Assessment
Reliability Graph with General Gates

ABSTRACT

The safety of nuclear power plants is analyzed by a probabilistic risk assessment, and the fault tree analysis is the most widely used method for a risk assessment with the event tree analysis. One of the well-known disadvantages of the fault tree is that drawing a fault tree for a complex system is a very cumbersome task. Thus, several graphical modeling methods have been proposed for the convenient and intuitive modeling of complex systems. In this paper, the reliability graph with general gates (RGGG) method, one of the intuitive graphical modeling methods based on Bayesian networks, is improved for the reliability analyses of dynamic systems that have various operation modes with time. A reliability matrix is proposed and it is explained how to utilize the reliability matrix in the RGGG for various cases of operation mode changes. The proposed RGGG with a reliability matrix provides a convenient and intuitive modeling of various operation modes of complex systems, and can also be utilized with dynamic nodes that analyze the failure sequences of subcomponents. The combinatorial use of a reliability matrix with dynamic nodes is illustrated through an application to a shutdown cooling system in a nuclear power plant.

1. Introduction

Various studies have been conducted for the development of safety analysis methods suitable for nuclear power plants. The fault tree analysis is the most widely used method for a reliability and safety evaluation in the field of safety engineering [1], and the safety of nuclear power plants is estimated using a probabilistic risk assessment method adopting

* *Corresponding author.*
E-mail address: phseong@kaist.ac.kr (P.H. Seong).

http://dx.doi.org/10.1016/j.net.2015.12.002

the fault tree analysis [2,3]. However, the construction of fault trees for large and complex systems is usually difficult, time-consuming, and susceptible to human errors. A fault tree may not follow a system diagram, and as a result, it may not be easy to relate the system flow to the logic that leads to a failure in the model [4]. Several methods such as the reliability graph with general gates (RGGG) [5], GO-FLOW [6], and various uses of Petri nets [7,8] have been proposed for a convenient and intuitive graphical modeling of complex systems and can be used as alternatives or complementary methods to the fault tree analysis.

The conventional fault tree method also has several difficulties in a reliability analysis of dynamic systems. In this paper, a dynamic system is defined as a system whose failure is dependent on the failure sequences of subcomponents and/or that have various operation modes with time. To analyze dynamic systems, various failure mechanisms with time requirements such as failure orders of the subcomponents and changes of the system states need to be modeled and quantitatively estimated. To overcome the limitations of the conventional static fault tree analysis and model dynamic systems, two types of dynamic fault trees have been developed: a dynamic fault tree with dynamic gates [9] and a dynamic fault tree with house events [10]. Dugan et al [9] proposed four dynamic gates to model dynamic systems whose failures are dependent on the failure sequence of the subcomponents. The proposed dynamic gates are a functional-dependency (FDEP) gate, spare gates [cold spare (CSP), hot spare (HSP), and warm spare (WSP)], a priority AND gate (PAND), and a sequence-enforcing (SEQ) gate. Cepin and Mavko [10] introduced house events and a house events matrix to the conventional fault tree to handle various operation modes and configuration changes with time.

Dynamic fault trees provide ways to analyze the reliability of dynamic systems, but they also cannot escape from the complexity of modeling fault trees which is the aforementioned shortcoming of the conventional static fault tree. In addition, it is not easy for dynamic fault trees to concurrently handle both dynamic features: sequentially dependent failures and operation mode changes with time.

Shin and Seong [11,12] developed a convenient dynamic modeling method using the RGGG by adding dynamic nodes (FDEP, Spare, PAND nodes) for the qualitative and quantitative analysis of dynamic systems whose failures depend on the failure sequence of the subcomponents. The RGGG is an improved reliability graph model developed for the intuitive modeling of a target system from its functional block diagram and paves the way for a convenient reliability analysis of complex systems [5].

In this paper, a reliability estimation method using the RGGG is proposed for an analysis of dynamic systems that have various operation modes with time by introducing a reliability matrix for the RGGG. The proposed method provides convenient and intuitive modeling of configuration changes of complex systems. In addition, both the dynamic features of sequentially dependent failures and operation mode changes can be analyzed at once using the dynamic nodes developed in works of Shin and Seong [11,12] in combination with the reliability matrix.

The remainder of this paper is structured as follows: The second section introduces briefly the RGGG and the dynamic fault tree with house events. The third section proposes the RGGG with a reliability matrix and explains how to utilize the reliability matrix in the RGGG for the various cases of configuration changes. The fourth section shows the applicability of the proposed method through an application to a simple electrical system that has various operation modes then, the reliability of a shutdown cooling system in a nuclear power plant is estimated using the RGGG with dynamic nodes and the reliability matrix in the fifth section. The sixth

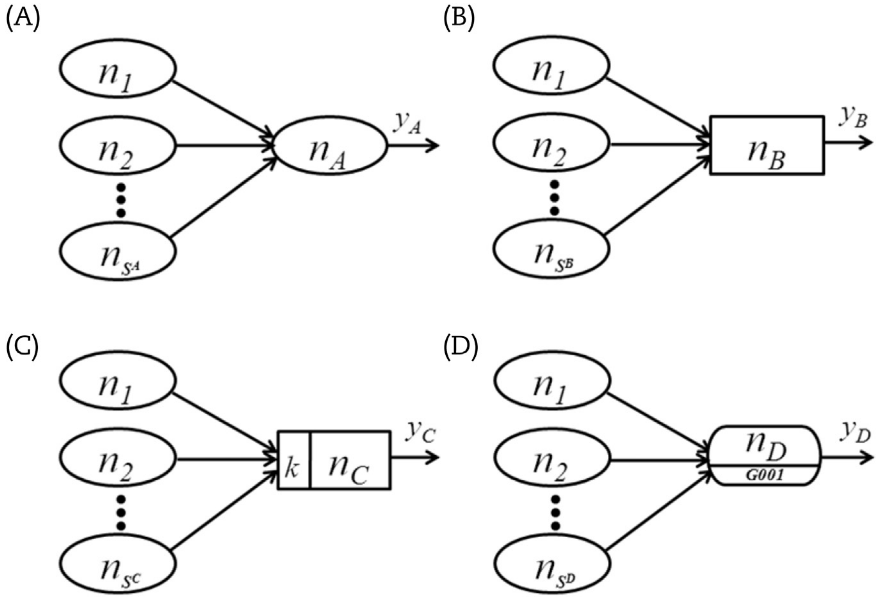


Fig. 1 – Definition of the nodes of the reliability graph with general gates. (A) OR node; (B) AND node; (C) *k*-out-of-*n* node; and (D) a general purpose node.

Table 1 – Probability table for an OR node with two inputs.

	$y_1 = 1$ (success)		$y_1 = 0$ (failure)	
	$y_2 = 1$ (success)	$y_2 = 0$ (failure)	$y_2 = 1$ (success)	$y_2 = 0$ (failure)
$y_A = 1$ (success)	$r_{1A} + r_{2A} - r_{1A}r_{2A}$	r_{1A}	r_{2A}	0
$y_A = 0$ (success)	$1 - (r_{1A} + r_{2A} - r_{1A}r_{2A})$	$1 - r_{1A}$	$1 - r_{2A}$	1

y_i: output of node i.
r_{ij}: reliability of arc from node i to node j.

section encompasses the discussion and conclusion of the proposed method.

2. Background

This section explains the RGGG method that is the basis of this study and the dynamic fault tree with house events developed to handle various operation modes.

2.1. RGGG

The reliability graph is an intuitive method of a reliability analysis that is able to model a system using a one-to-one match graph [13,14]. However, reliability graphs are not widely used because they have a low capability of expression; they can only express the characteristics of an OR gate. To overcome the limited capability of expression, the RGGG was proposed with additional general gates (nodes). The RGGG suffers no loss of intuitiveness and has the advantages of a conventional reliability graph. Fig. 1 shows the general nodes (OR, AND, *k*-out-of-*n*, and a general purpose node) that are utilized in the RGGG.

To calculate the system reliability through the RGGG, the RGGG is converted into an equivalent Bayesian network by determining the probability tables of all the nodes. A Bayesian network is a probabilistic graphical model that represents a set of random variables and their conditional dependencies, and it has been used for a reliability analysis of complex systems [15,16]. For example, Table 1 shows the probability table of an OR node n_A with two inputs from node n_1 and n_2 in the RGGG. A detailed explanation of how to construct a probability table for each node can be found in works of Kim and Seong [5]. In addition to expressing the OR, AND, and *k*-out-of-*n* gates, a gate with any characteristic can be expressed by determining the corresponding probability table.

The failure scenario of a target system can be modeled with an RGGG that has a very similar shape to the real system and the signal flow or fluid flow can be expressed very intuitively in the RGGG. In conclusion, as the RGGG can be constructed directly from the real structure or functional block diagram of the target system and represent a signal flow intuitively, it has many merits in analyzing the reliability of complex systems. The calculation result of the RGGG does not have truncation errors that generally occur in the minimal cut set (MCS) based fault tree analyzing complex systems. The RGGG has been used in various ways [17–19] and was recently improved to analyze the reliability of dynamic systems whose failures depend on the failure sequence of the subcomponents [11,12].

2.2. Dynamic fault tree with house events

To extend the conventional fault tree with the time requirements and evaluate the actual time dependent profile of nuclear power plant risk, a dynamic fault tree with house events was developed by Cepin and Mavko [10]. The house events are used primarily to switch on and off the respective parts of the integrated fault tree. The house events table is introduced to document which house events are switched on and off for a certain fault tree top event to suit its respective function event in its appropriate scenario branch. Cepin and Mavko utilized house events to extend the classic fault tree with time. The input of the house events status is achieved through the house events matrix:

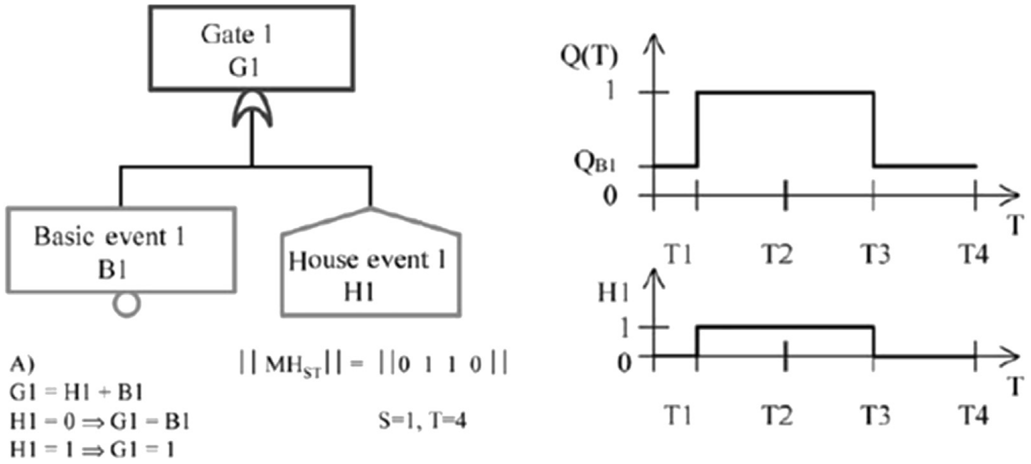
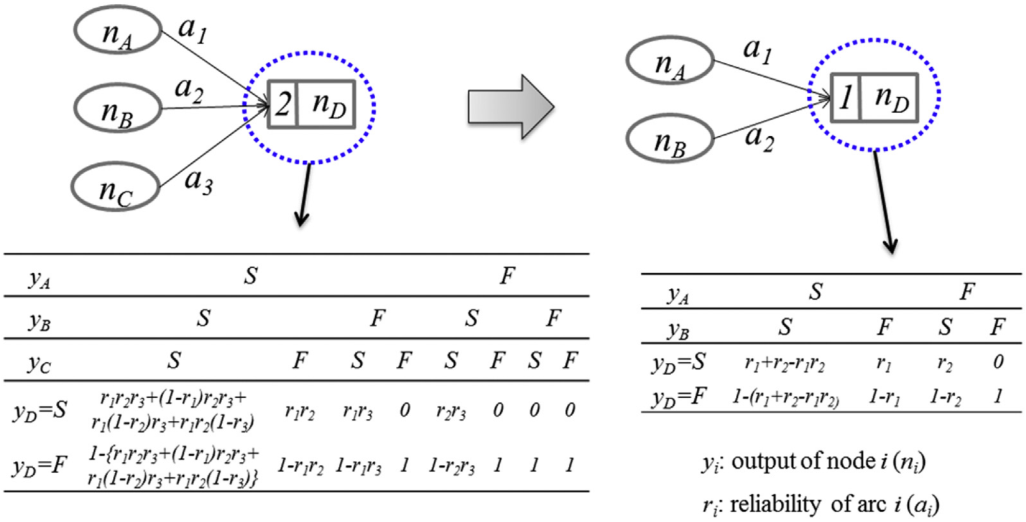


Fig. 2 – A dynamic fault tree with house events for an equipment outage.



y_A	S				F			
y_B	S		F		S		F	
y_C	S	F	S	F	S	F	S	F
y_D=S	$r_1r_2r_3+(1-r_1)r_2r_3+$ $r_1(1-r_2)r_3+r_1r_2(1-r_3)$	r_1r_2	r_1r_3	0	r_2r_3	0	0	0
y_D=F	$1-\{r_1r_2r_3+(1-r_1)r_2r_3+$ $r_1(1-r_2)r_3+r_1r_2(1-r_3)\}$	$1-r_1r_2$	$1-r_1r_3$	1	$1-r_2r_3$	1	1	1

y_A	S		F	
y_B	S	F	S	F
y_D=S	$r_1+r_2-r_1r_2$	r_1	r_2	0
y_D=F	$1-(r_1+r_2-r_1r_2)$	$1-r_1$	$1-r_2$	1

y_i: output of node i (n_i)

r_i: reliability of arc i (a_i)

Fig. 3 – Modification of the structure of the reliability graph with general gates and the probability table.

$$\|MH_{ST}\| = \left\| \begin{matrix} H_{11} & H_{12} & \cdots & H_{1T} \\ H_{21} & \cdots & & \\ \cdots & & H_{ST} & \cdots \\ H_{S1} & \cdots & & H_{ST} \end{matrix} \right\| \tag{1}$$

MH_{ST} refers to the house events matrix and H_{st} refers to the house event value (true or false) for house event s at time t. The house events matrix is a representation of house events switched on and off through the discrete points of time. The number of rows in the house events matrix represents a number of those house events in the model, and the number of columns represents the number of time periods in which mutually different system configurations exist. The quantitative analysis is achieved by finding the minimal cut sets of fault trees in each time point. Fig. 2 shows a use of the house events matrix in the modeling of an equipment outage. The house event under an OR gate serves to model an outage of equipment modeled in a gate or basic event under the mentioned OR gate. With house event 1 (H1) set to 1 (true), gate 1 (G1) is 1 (true) independent of basic event 1 (B1), which indicates the outage of equipment modeled in B1. The time diagram explains the house events matrix that simulates the outage of equipment modeled in B1 for time points T2 and T3.

The main advantage of the dynamic fault tree with house events is that no additional knowledge of other methods is needed; only the use of the conventional fault tree is extended. The existing fault tree models can be used and updated with the additional house events, which enable distinguishing configurations in their respective time points. In addition, applications of the dynamic fault tree include optimization of parameters in probabilistic models to minimize the overall risk, such as the configuration control.

3. RGGG with reliability matrix

The dynamic fault tree was proposed by introducing house events and a house events matrix to the conventional fault tree, but the fault tree itself has a shortcoming in regards to the difficulty in modeling complex systems. In this section, the conventional RGGG, which is an intuitive graphical modeling method, is extended to handle various operation modes. For a reliability analysis of the dynamic systems whose configuration changes according to various operation modes with time, more than one or even many conventional RGGGs are required in proportion to the number of operation modes. If the structure of the RGGG changes, the probability table of each node also should be modified according to the failure mechanism of each operation mode for quantitative reliability estimation. For example, as shown in Fig. 3, if the trip logic of a control system in a nuclear power plant is changed from 2-out-of-3 voting logic to 1-out-of-2 due to a surveillance test, the structure of the RGGG for the control system should be revised according to each operation mode including the probability table of the node n_D.

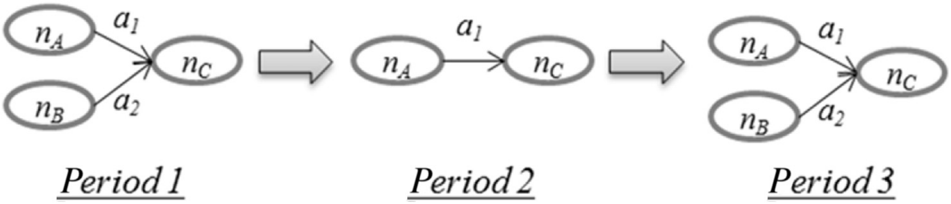


Fig. 4 – Change in the number of inputs to the OR node.

Table 2 – Probability table for the OR node in Period 1 of Fig. 4.

	$y_A = 1$		$y_A = 0$	
	$y_B = 1$	$y_B = 0$	$y_B = 1$	$y_B = 0$
$y_C = 1$	$r_{11} + r_{21} - r_{11}r_{21}$	r_{11}	R_{21}	0
$y_C = 0$	$1 - (r_{11} + r_{21} - r_{11}r_{21})$	$1 - r_{11}$	$1 - r_{21}$	1

Table 3 – Probability table for the OR node in Period 2 of Fig. 4.

	$y_A = 1$		$y_A = 0$	
	$y_B = 1$	$y_B = 0$	$y_B = 1$	$y_B = 0$
$y_C = 1$	r_{12}	r_{12}	0	0
$y_C = 0$	$1 - r_{12}$	$1 - r_{12}$	1	1

Table 4 – Probability table for the OR node in Period 3 of Fig. 4.

	$y_A = 1$	$y_A = 0$
$y_C = 1$	r_{12}	0
$y_C = 0$	$1 - r_{12}$	1

As house events and a house events matrix are used in a dynamic fault tree to reflect several fault trees, a reliability matrix is proposed for one RGGG to express various system operation modes varying with time. To keep the advantage of the RGGG method to model a system by using a one-to-one match graph from the functional block diagram, additional nodes functioning as the house events in the dynamic fault tree are not employed in the RGGG. Only the reliability matrix is newly introduced to the conventional RGGG to handle the changes of the operation modes. The reliability matrix for the arcs in the RGGG has a very similar shape to the house events matrix in the dynamic fault tree, and is constructed as follows:

$$\|RM_{at}\| = \left\| \begin{matrix} r_{11} & r_{12} & \cdots & r_{1T} \\ r_{21} & \cdots & & \\ \cdots & & r_{nt} & \cdots \\ r_{N1} & \cdots & & r_{NT} \end{matrix} \right\| \tag{2}$$

The variable r_{nt} in the reliability matrix refers to the reliability of arc a_n at time t. The variables N and T refer to the number of arcs and time periods, respectively. Therefore, the number of rows in the matrix represents a number of arcs in the RGGG that are modeling various operation modes as a function of time. The number of columns represents the number of time periods in which mutually different system configurations exist. By determining the reliability of each arc according to the system configuration during each period, the various operation modes varying with time can be modeled with one RGGG. In other words, the change of arc probabilities has the same effect as modifying the structure of the RGGG and the probability tables in the RGGG. The following sections describe how to utilize the reliability matrix in the RGGG for various cases of the configuration changes in detail.

3.1. *Change in the number of inputs*

The reliability matrix can be used for the RGGG to express a component that is not considered during a certain period for a reason such as routine maintenance. As shown in Fig. 4, it is assumed that the equipment modeled in arc a_2 which is an input of the OR node is not considered in the model during Period 2. The probability table for node n_C during Period 1 is shown in Table 2. If r_{11} and r_{21} in Table 2 are revised into r_{12} and 0 respectively, the probability table is changed into Table 3, which describes node n_C during Period 2. As the probabilities in Table 3 have no relation to the output of node n_B, the probability table is the same as Table 4, which is for the OR node with one input during Period 2. That is, the reliability of a component, which is not considered during a certain

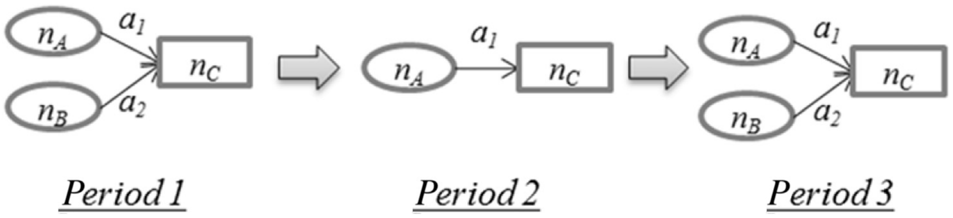


Fig. 5 – Change in the number of inputs to the AND node.

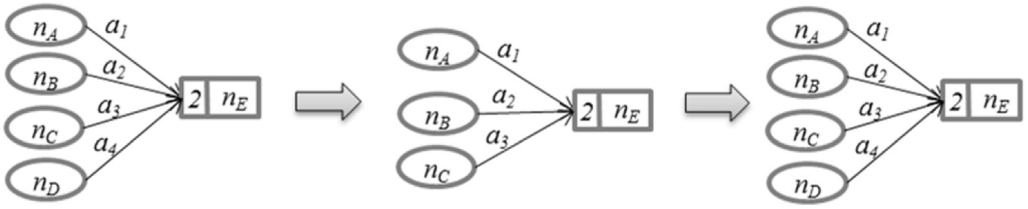


Fig. 6 – Change of 2-out-of-4 voting logic to 2-out-of-3 and change back to 2-out-of-4.

Table 5 – Probability table for the 2-out-of-4 node in Period 1 of Fig. 6.

y_A	1								0							
y_B	1				0				1				0			
y_C	1		0		1		0		1		0		1		0	
y_D	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
$y_E = 1$	$r_1r_2r_3r_4 + (1-r_1)r_2r_3r_4 + r_1(1-r_2)r_3r_4 + r_1r_2(1-r_3)r_4 + r_1r_2r_3(1-r_4) + (1-r_1)(1-r_2)r_3r_4 + (1-r_1)r_2(1-r_3)r_4 + (1-r_1)r_2r_3(1-r_4) + r_1(1-r_2)(1-r_3)r_4 + r_1(1-r_2)r_3(1-r_4) + r_1r_2(1-r_3)(1-r_4)$	$r_1r_2r_3 + (1-r_1)r_2r_3 + r_1(1-r_2)r_3 + r_1r_2(1-r_3)$	$r_1r_2r_4 + (1-r_1)r_2r_4 + r_1(1-r_2)r_4 + r_1r_2(1-r_4)$	r_1r_2	$r_1r_3r_4 + (1-r_1)r_3r_4 + r_1(1-r_3)r_4 + r_1r_3(1-r_4)$	r_1r_3	r_1r_4	0	$r_2r_3r_4 + (1-r_2)r_3r_4 + r_2(1-r_3)r_4 + r_2r_3(1-r_4)$	r_2r_3	r_2r_4	0	r_3r_4	0	0	0
$y_E = 0$	$1 - \{r_1r_2r_3r_4 + (1-r_1)r_2r_3r_4 + r_1(1-r_2)r_3r_4 + r_1r_2(1-r_3)r_4 + r_1r_2r_3(1-r_4) + (1-r_1)(1-r_2)r_3r_4 + (1-r_1)r_2(1-r_3)r_4 + (1-r_1)r_2r_3(1-r_4) + r_1(1-r_2)(1-r_3)r_4 + r_1(1-r_2)r_3(1-r_4) + r_1r_2(1-r_3)(1-r_4)\}$	$1 - \{r_1r_2r_3 + (1-r_1)r_2r_3 + r_1(1-r_2)r_3 + r_1r_2(1-r_3)\}$	$1 - \{r_1r_2r_4 + (1-r_1)r_2r_4 + r_1(1-r_2)r_4 + r_1r_2(1-r_4)\}$	$1 - r_1r_2$	$1 - \{r_1r_3r_4 + (1-r_1)r_3r_4 + r_1(1-r_3)r_4 + r_1r_3(1-r_4)\}$	$1 - r_1r_3$	$1 - r_1r_4$	1	$1 - \{r_2r_3r_4 + (1-r_2)r_3r_4 + r_2(1-r_3)r_4 + r_2r_3(1-r_4)\}$	$1 - r_2r_3$	$1 - r_2r_4$	1	$1 - r_3r_4$	1	1	1

Table 6 – Probability table for the 2-out-of-3 node in Period 2 of Fig. 6.

y_A	1								0							
y_B	1				0				1				0			
y_C	1		0		1		0		1		0		1		0	
y_D	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
$y_E = 1$	$r_1r_2r_3 + (1-r_1)r_2r_3 + r_1(1-r_2)r_3 + r_1r_2(1-r_3)$	$r_1r_2r_3 + (1-r_1)r_2r_3 + r_1(1-r_2)r_3 + r_1r_2(1-r_3)$	r_1r_2	r_1r_2	r_1r_3	r_1r_3	0	0	r_2r_3	r_2r_3	0	0	0	0	0	0
$y_E = 0$	$1 - \{r_1r_2r_3 + (1-r_1)r_2r_3 + r_1(1-r_2)r_3 + r_1r_2(1-r_3)\}$	$1 - \{r_1r_2r_3 + (1-r_1)r_2r_3 + r_1(1-r_2)r_3 + r_1r_2(1-r_3)\}$	$1 - r_1r_2$	$1 - r_1r_2$	$1 - r_1r_3$	$1 - r_1r_3$	1	1	$1 - r_2r_3$	$1 - r_2r_3$	1	1	1	1	1	1

Table 7 – Probability table for the 2-out-of-3 node with three inputs.

y_A	1				0			
y_B	1		0		1		0	
y_C	1	0	1	0	1	0	1	0
$y_E = 1$	$r_1r_2r_3 + (1-r_1)r_2r_3 + r_1(1-r_2)r_3 + r_1r_2(1-r_3)$	r_1r_2	r_1r_3	0	r_2r_3	0	0	0
$y_E = 0$	$1 - \{r_1r_2r_3 + (1-r_1)r_2r_3 + r_1(1-r_2)r_3 + r_1r_2(1-r_3)\}$	$1 - r_1r_2$	$1 - r_1r_3$	1	$1 - r_2r_3$	1	1	1

period, is set to 0 during that period in the reliability matrix. The reliability matrix for only arc a_2 in Fig. 4 is as follows:

$$\|\mathrm{RM}_{at}\| = \| r_{21} \quad 0 \quad r_{23} \| \tag{3}$$

In a similar manner, the change in the number of inputs to the AND node can be expressed using the reliability matrix. Fig. 5 shows that a component modeled in arc a_2, which is an input of AND node, is not considered in the model during Period 2. The difference with the OR node is that the output of node n_B and the reliability of arc a_2 are set to 1 during Period 2, and thus only arc a_1 is considered as an input of node n_C. The reliability matrix only for arc a_2 in Fig. 5 is as follows:

$$\|\mathrm{RM}_{at}\| = \| r_{21} \quad 1 \quad r_{23} \| \tag{4}$$

3.2. *Change of k-out-of-n logic*

Redundant channels are often employed in standby critical systems for safety critical applications [20]. The *k*-out-of-*n* logic is a widely adopted configuration for trip signal generations in nuclear power plants, and the trip logic changes during surveillance tests such as sensor and channel tests. For example, a 2-out-of-4 voting system for tripping the reactor during normal operation becomes either 2-out-of-3 or 1-out-of-3 logic during a surveillance test of a channel. In other words, as *n* decreases to (*n*−1) during a channel test, *k* may remain the same or may decrease to (*k*−1). In the former case, the unavailability of the trip system increases compared to the normal operation mode. In the latter case, the probability of a spurious trip increases compared to normal operation mode. The higher unavailability of the trip system is a serious safety-related defect because the plant may not be protected if the trip system fails during an emergency condition. The higher probability of a spurious trip entails high costs for a utility due to the interruption of plant operation and the expenses related to the restart of the plant. Since each change of the voting logic has its merits and faults, the value of *k* should be determined under careful consideration of plant safety and economic feasibility [21].

For the *k*-out-of-*n* voting system to operate normally at least *k* channels should be in normal state and the failure of more than (*n*−*k*) channels leads the voting system to a failure state. Therefore, for the reliability and availability analysis of a *k*-out-of-*n* voting system, the (*n*−*k*+1)-out-of-*n* gate is used in the fault tree modeling and *k*-out-of-*n* node is utilized in the RGGG method. The remaining part of this section describes how the reliability matrix can be applied to each change of value of *k*.

3.2.1. *Change from k-out-of-n to k-out-of-(n−1)*

If the value of k does not change even though n decreases by 1 due to a channel test, the unavailability of the voting system increases, while the probability of a spurious operation of the system decreases. The example voting system shown in Fig. 6 operates with 2-out-of-4 voting logic normally and operates with 2-out-of-3 voting logic during Period 2 due to a test of the channel modeled in arc a_4. From a reliability standpoint, this case can be understood as that the channel under testing breaks down and cannot transmit an operation signal when needed. In other words, if the channel modeled in arc a_4 in Fig. 6 is assumed to break down during Period 2, at least two operating signals from the other three channels are needed for the 2-out-of-4 voting system to operate, which is the same as the 2-out-of-3 voting system. Therefore, for a reliability analysis of the voting system, the reliability of the channel modeled in arc a_4 is set to 0 during the test in the reliability matrix. The reliability matrix only for arc a_4 in Fig. 6 is as follows:

$$\|\mathrm{RM}_{at}\| = \| r_{41} \quad 0 \quad r_{43} \| \tag{5}$$

The probability table for node n_E during Period 1 is shown in Table 5. The values of t of r_{nt} are omitted in the table for brevity. If r_{11}, r_{21}, r_{31}, and r_{41} in Table 5 are revised into r_{12}, r_{22}, r_{32}, and 0 respectively, the probability table is changed into Table 6, which describes node n_D during Period 2. As the probabilities in Table 6 have no relation to the output of node n_D, the probability table is the same as Table 7, which is for the 2-out-of-3 node with three inputs.

3.2.2. *Change from k-out-of-n to (k-1)-out-of-(n-1)*

This case describes the decrease of *k* by 1 with a decreasing value of *n*, which leads to a higher probability of spurious operation and a lower unavailability of the voting system compared to the normal operation mode. Fig. 7 shows an example of a decreasing value of *k* during a certain period. The example system operates with 2-out-of-4 voting logic normally and operates with 1-out-of-3 voting logic during a test of a channel modeled in arc a_4. In this case, from a reliability standpoint, the decrease of *k* can be understood as the channel under testing always transmitting an operating signal during the test. In other words, if the 2-out-of-4 voting system in Fig. 7 is assumed to always receive one operating signal through a channel under testing, only one more signal from the other three channels is needed for the system to operate, which is the same as a 1-out-of-3 voting system. Therefore, for a reliability analysis of the voting system, the output of node

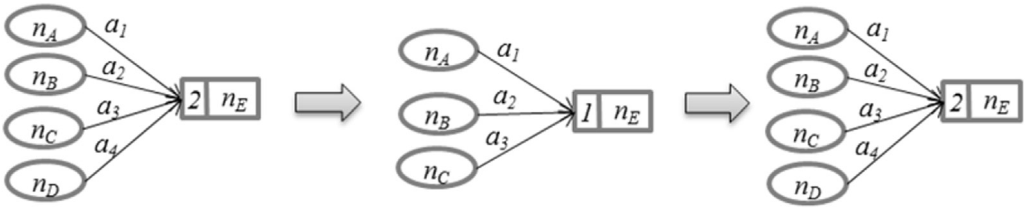


Fig. 7 – Change of 2-out-of-4 voting logic to 1-out-of-3 and change back to 2-out-of-4.

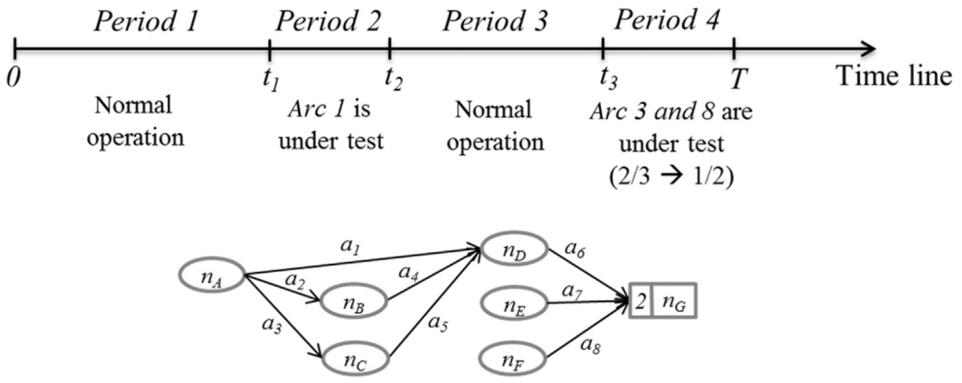


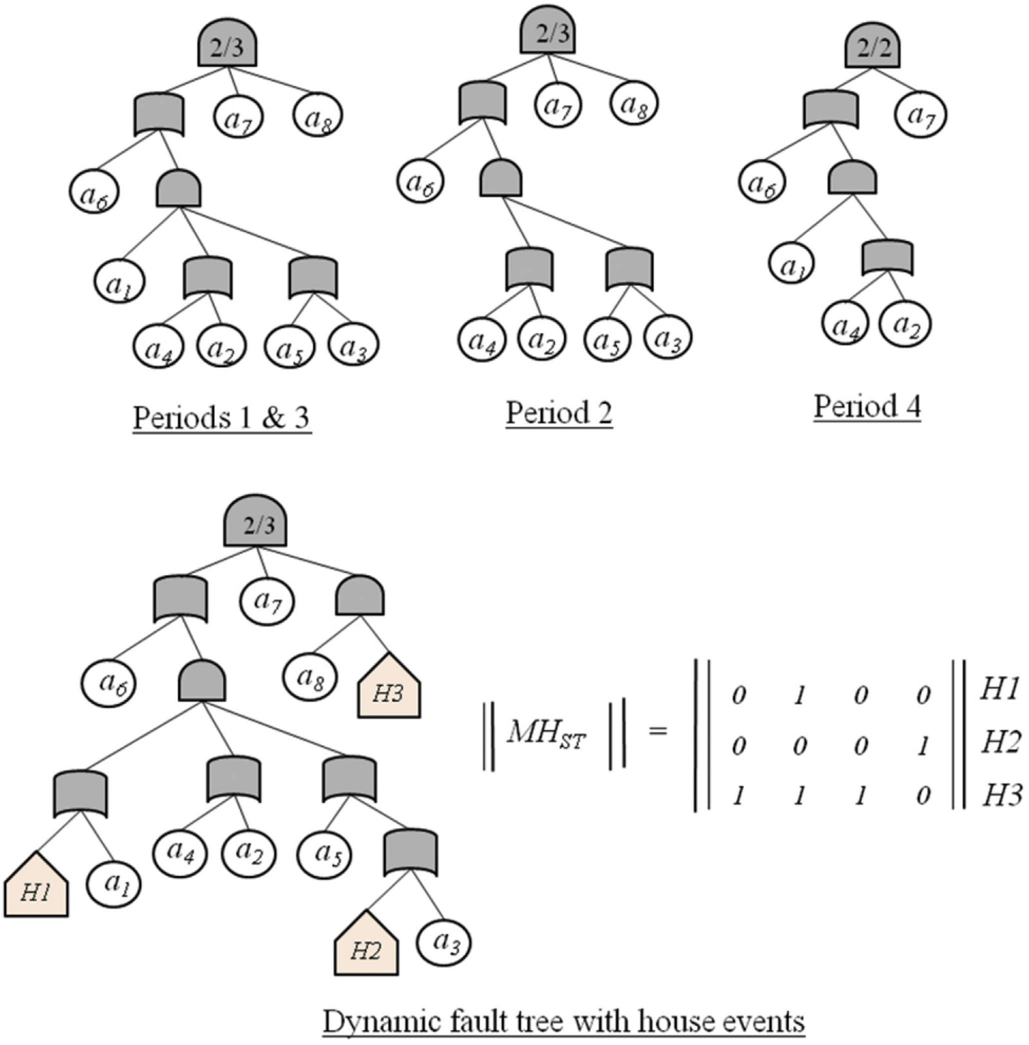
Fig. 8 – Reliability graph with general gates for the hypothetical system that has four operating periods.

n_D and the reliability of the channel modeled in arc a_4 are set to 1 during the test in the reliability matrix. The reliability matrix for only arc a_4 in Fig. 7 is as follows:

$$\|RM_{at}\| = \| r_{41} \quad 1 \quad r_{43} \| \tag{6}$$

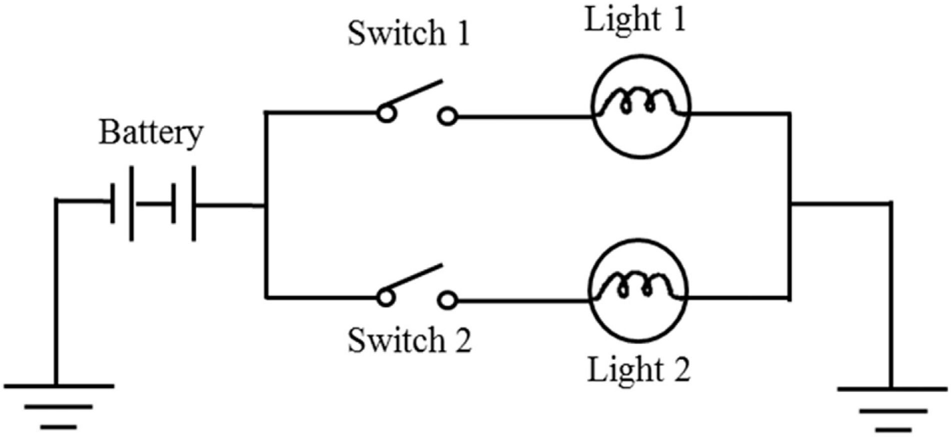
3.3. *Application to a hypothetical system*

In this section, the proposed RGGG method with the reliability matrix is applied to model a hypothetical system which has three operation modes during the total process time. The RGGG for the system is shown in Fig. 8. Signals flow from left



$$\| MH_{ST} \| = \begin{Vmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{Vmatrix} \begin{matrix} H1 \\ H2 \\ H3 \end{matrix}$$

Fig. 9 – Dynamic fault tree for the hypothetical system that has four operating periods.



Time point	Operation mode
1	Initial time
2	Battery is connected
3	Switch S1 is commanded to close
4	10 h after Time point 3
5	Switch S2 is commanded to close
6	10 h after Time point 5

Fig. 10 – An electrical system which has six points of operation mode changes.

to right and the components modeled in nodes n_B, n_C, and n_D need at least one input signal to generate an output signal and the component modeled in node n_G needs at least two inputs to generate an output. The system has four operation modes during the total process time. During Periods 1 and 3, the system operates normally and the channel modeled in arc a_1 is under testing during Period 2. The channels modeled in arcs a_3 and a_8 are under testing during Period 4 and in the meantime the component modeled in Node n_G has 1-out-of-2 voting logic. For a reliability analysis of the system using fault tree modeling, each operation mode should be described by each fault tree, but only one dynamic fault tree with house events and a house events matrix can be used for describing all the operation modes as shown in Fig. 9. The basic event a_i in Fig. 9 refers to a failure of the channel modeled in arc a_i. The various system operation modes during the total process time can also be modeled using the RGGG shown in Fig. 8 which represents the normal operation mode by utilizing the proposed reliability matrix. The reliability matrix for the example system is as follows:

$$\|RM_{at}\| = \left\| \begin{matrix} r_{11} & 0 & r_{13} & r_{14} \\ r_{31} & r_{32} & r_{33} & 0 \\ r_{81} & r_{82} & r_{83} & 1 \end{matrix} \right\| \tag{7}$$

The rows for the channels that are not affected by the change of operation mode are omitted in the reliability matrix. As the channel modeled in arc a_1 is not considered in the system during Period 2 due to a channel test and arc a_1 is an

Table 8 – Description of the probabilities for the component in the electrical system.

Parameter	Value	Description
P_B	0.9	Probability that the battery works normally
P_P	0.1	Probability that a switch is prematurely closed
P_S	0.7	Probability that a switch becomes closed normally
P_L	0.8	Probability that a light bulb starts to work normally
λ_L	0.001/hr	Probability of failure per hr of a light bulb during lighting

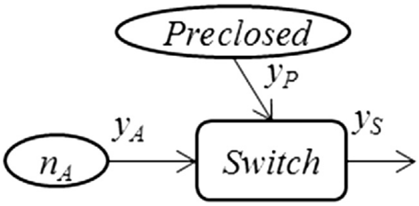


Fig. 11 – A novel node for a switch which could be prematurely closed.

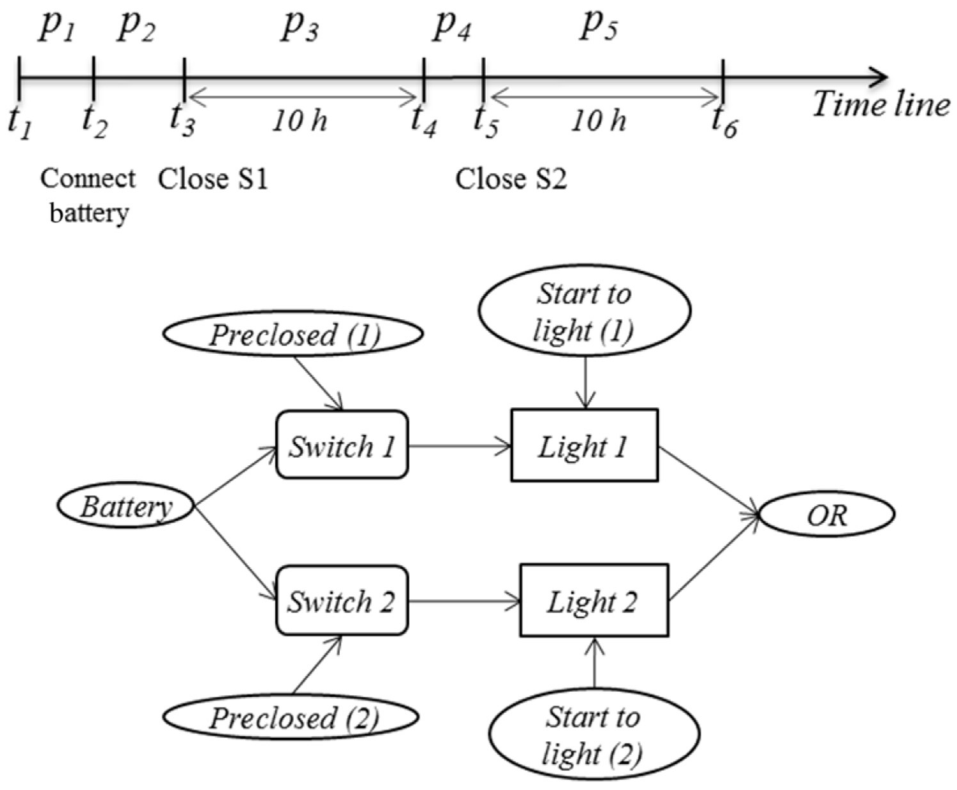
Table 9 – Probability table for the node of the switch which could be prematurely closed.

	$y_A = 1$		$y_A = 0$	
	$y_P = 1$	$y_P = 0$	$y_P = 1$	$y_P = 0$
$y_S = 1$	1	P_S	0	0
$y_S = 0$	0	$1 - P_S$	1	1

input of OR node n_D, the value of r_{12} is set to 0 in the reliability matrix. By the same logic, the value of r_{34} is set to 0 in the reliability matrix. During Period 4, with a test of the channel modeled in arc a_8, the voting logic of the component modeled in node n_G changes from k-out-of-n to (k–1)-out-of-(n–1). Therefore, the value of r_{84} is set to 1 in the reliability matrix. In conclusion, the reliabilities of the example system, which has four operating periods with three operation modes, can be estimated by the one RGGG in Fig. 8 and the reliability matrix in Eq. (7). In other words, the revision of the RGGG structure and the probability tables according to each operation mode are unnecessary. Furthermore, the actual structure and signal flows in the system are easily comprehensible from the RGGG compared to the fault tree with house events as shown in Figs. 9 and 10.

4. Applicability of the proposed method

The RGGG method provides a convenient graphical modeling from functional block diagrams of complex systems including a quantitative reliability estimation using Bayesian networks. One of the advantages of the RGGG is a wide applicability to various systems by utilizing general nodes with adequate probability tables that represent system failure logic. In other words, a node in the RGGG can be used to describe various causal relations between events that are not limited to OR and AND relations. In this section, the applicability of the proposed RGGG with a reliability



$$\|RM_{at}\| = \begin{array}{c|ccccc|l} & p_1 & p_2 & p_3 & p_4 & p_5 & \\ & 0 & 0.9 & 0.9 & 0.9 & 0.9 & \text{Battery} \\ & 0 & 0 & 0.7 & 0.7 & 0.7 & \text{Switch 1} \\ & 0 & 0 & 0 & 0 & 0.7 & \text{Switch 2} \end{array}$$

Fig. 12 – The reliability graph with general gates with a reliability matrix for the electrical system.

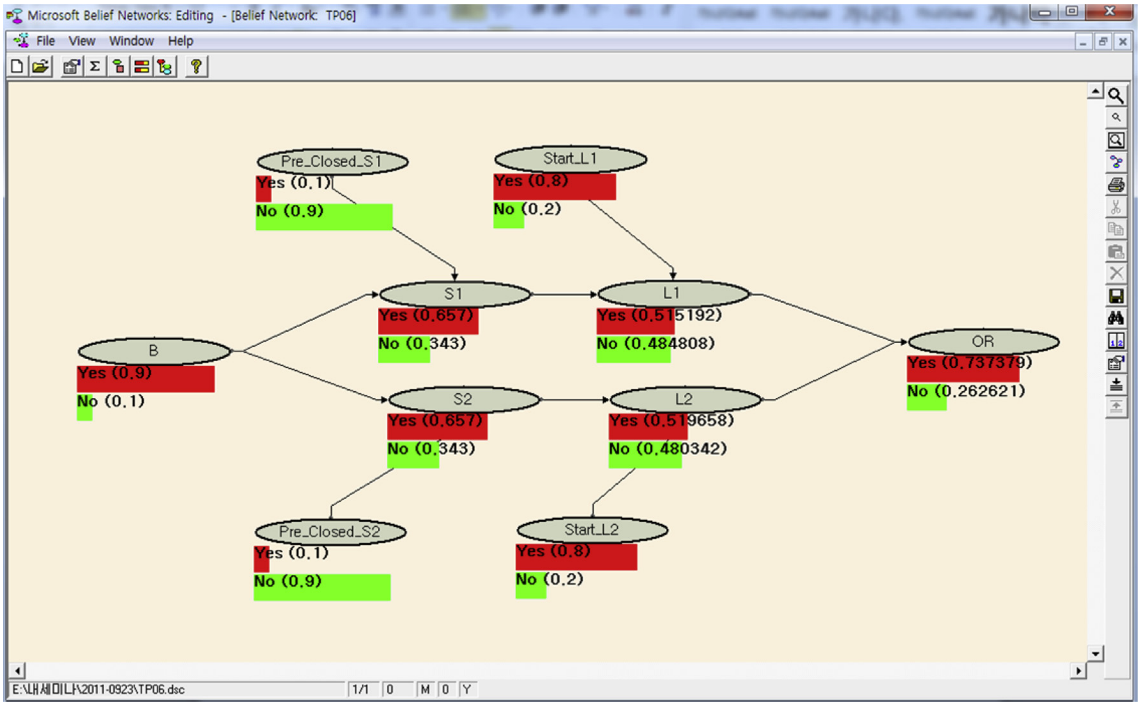


Fig. 13 – Evaluation result of the electrical system at Time Point 6.

matrix is verified by applying a simple electrical system which was treated by Matsuoka and Kobayashi [6] using the GO-FLOW method.

The electrical system shown in Fig. 10 has six time points at which the operation mode changes. Time Point 1 is the initial time the battery is connected at Time Point 2. Switch S1 is required to be closed at Time Point 3, and Time Point 4 is 10 hours after Time Point 3. At Time Point 5, which immediately succeeds Time Point 4, Switch S2 is required to be closed and Time Point 6 is 10 hours after Time Point 5. Table 8 explains the probabilities for the components in the electrical system. The probabilities of P_P and P_S apply to both Switches 1 and 2, and the probabilities of P_L and λ_L apply to both Lights 1 and 2. The switches in the system could be prematurely closed before the closure requirement with a probability of P_p. As the existing nodes such as OR and AND nodes cannot describe this logic, a novel node for the switches is developed as shown in Fig. 11. Node n_A has an output of 1 when it transmits a flow of electricity to the switch; otherwise, it has an output of 0. The node "Preclosed" has an output of 1 when the switch is prematurely closed before the requirement to be closed, and has an output of 0 when the switch is not closed prematurely. The probability table for the node of the switch in Fig. 11 can be determined in Table 9. If the switch is prematurely closed when an electrical current is transmitted from Node n_A (y_A=1 and y_P=1), the probability that the current passes the switch is 1. On the other hand, if the switch is not prematurely closed when a current is transmitted from node n_A (y_A=1 and y_P=0), the probability that the current passes the switch is the same as the probability that the switch becomes closed at that time (P_S). With the developed nodes for the switches that can be prematurely closed, the RGGG for the electrical system is constructed with a reliability matrix as shown in Fig. 12. The RGGG is for estimating the probability that at least one light bulb is lit at each time point. As a light bulb has the probability of "Start to light" in addition to the failure probability during lighting, the node "Start to light" is used and the connected light bulb starts to work only when both inputs from the nodes "Switch" and "Start to light" are available. The reliability matrix for the system is determined according to the operation mode during each operation period, and the rows for the nodes, which are not affected by the change of operation mode, are omitted in the reliability matrix shown in Fig. 12. The quantitative analysis to estimate the reliability of the electrical system at each time point is conducted using MSBNx which is a noncommercial software tool for evaluating Bayesian networks [22]. A screenshot of the evaluation result at Time Point 6 using the MSBNx is shown in Fig. 13. The probability that at least one light bulb is lit appears in the OR node and the probability that each light bulb is lit is shown in the node for each light bulb. The evaluation results at all time points are shown in Table 10 and the results are the same as that of the GO-FLOW method [6].

Table 10 – Evaluation results at all the time points.

	Reliability of the electrical system
Time Point 1	0
Time Point 2	0.13824
Time Point 3	0.55555
Time Point 4	0.55044
Time Point 5	0.74177
Time Point 6	0.73738

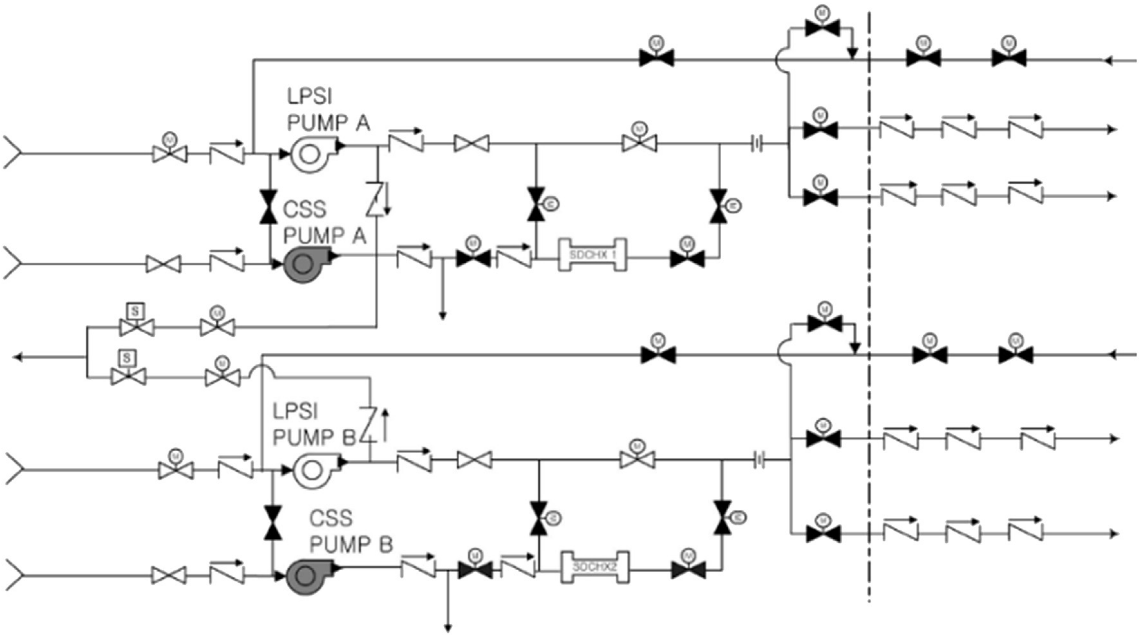
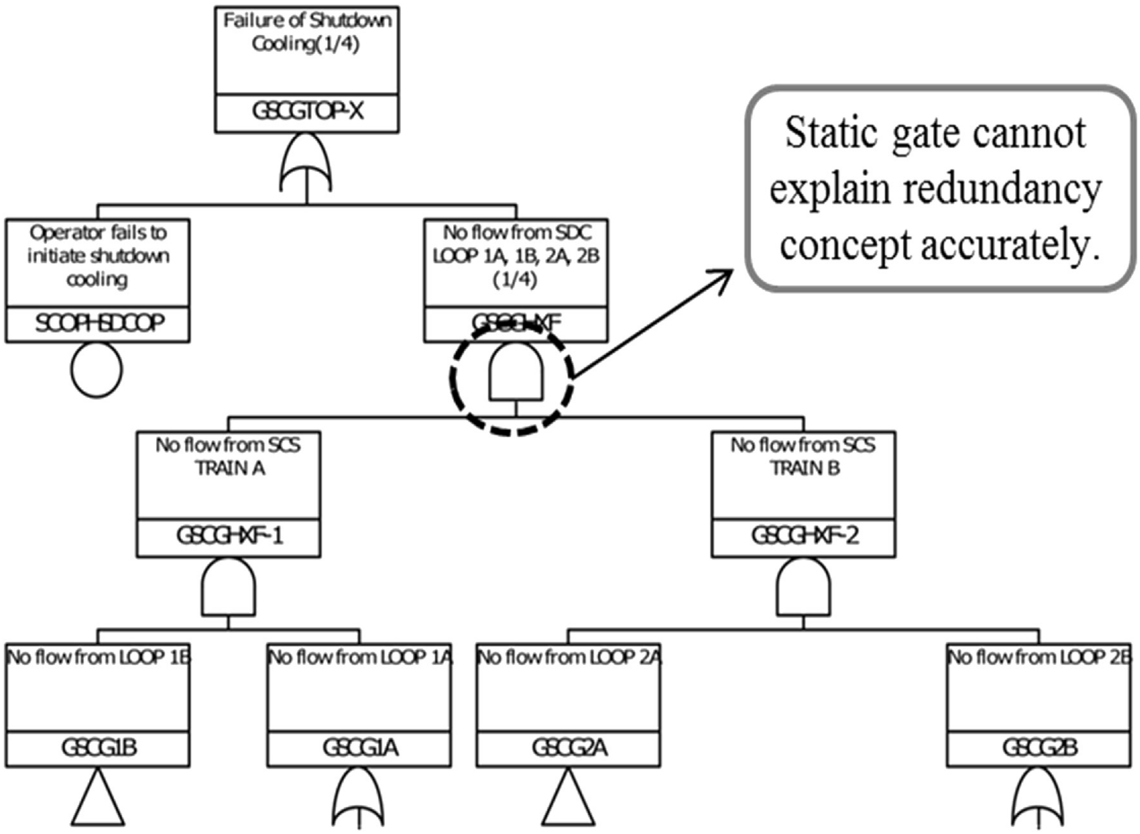


Fig. 14 – Simplified diagram for the shutdown cooling system. CSS, containment spray system; LPSI, low pressure safety injection.



Static gate cannot explain redundancy concept accurately.

Fig. 15 – Upper part of the fault tree for the shutdown cooling system. SCS, shutdown cooling system; SDC, shutdown cooling.

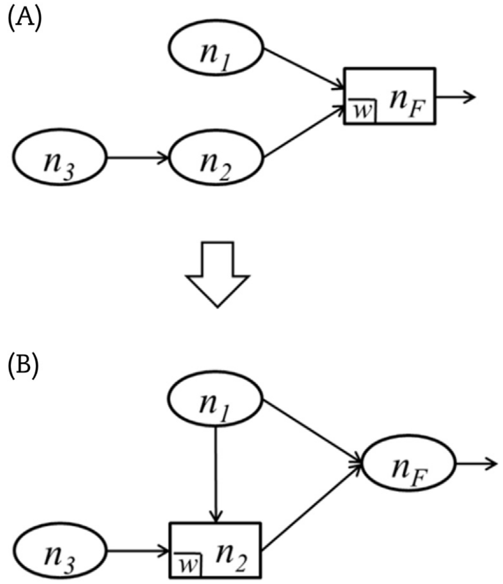


Fig. 16 – Spare nodes for dynamic reliability graph with general gates. (A) Original spare node. (B) Modified spare node.

5. Reliability Estimation of a Shutdown Cooling System

A nuclear power plant during the low power and shutdown (LPSD) period experiences various plant configurations and operational states [23]. There has been few probabilistic safety assessments (PSAs) for a whole LPSD period since the difficulty and cost for these assessments are considerable when compared with a PSA at full-power mode. A whole LPSD period is usually partitioned with several plant operational states (POSs) in which it is usually assumed that a nuclear power plant in a single POS has identical system configurations. For a detailed risk calculation, the POSs needed in the LPSD period may be increased to almost 20 POSs. In this section, the reliability of a shutdown cooling system (SCS) that has various operation modes during the LPSD period is analyzed using the proposed dynamic RGGG with a reliability matrix and dynamic nodes.

5.1. *Dynamic behaviors of a shutdown cooling system*

The function of the SCS is residual heat removal after a reactor shutdown. If the safety function of the SCS fails, then the coolant in the reactor vessel will boil and the nuclear fuel might be damaged. The SCS consists of two trains, and each train has enough capability for cooling the residual heat. The simplified

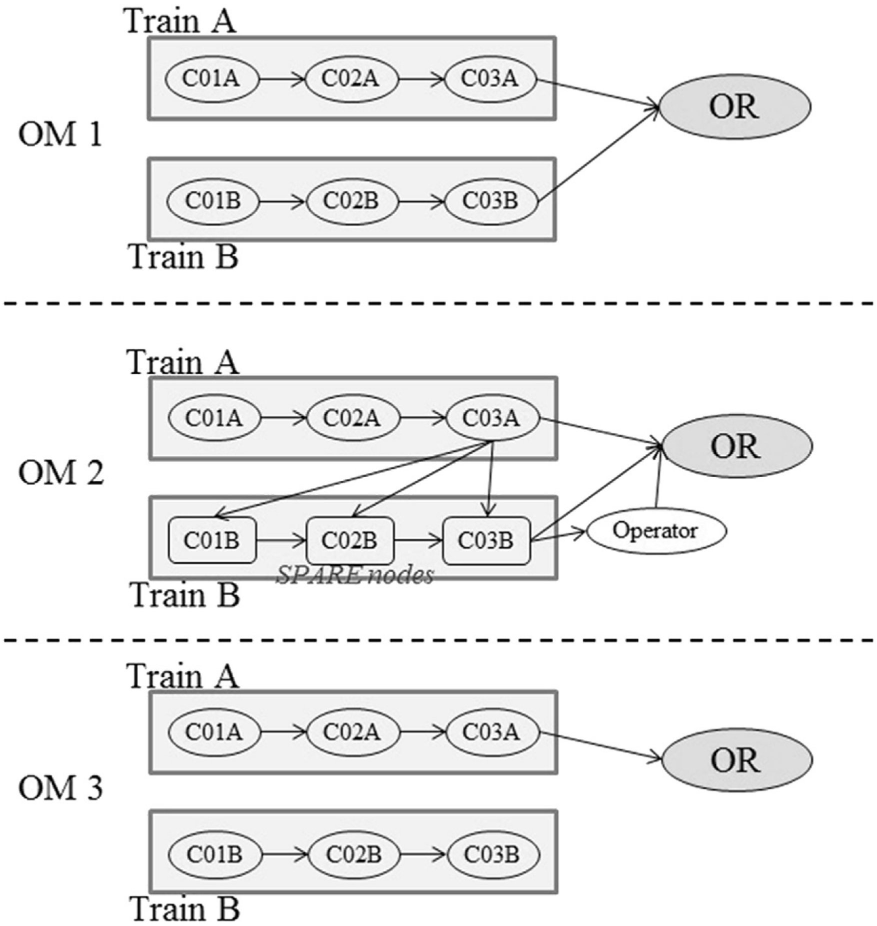


Fig. 17 – Simplified dynamic reliability graph with general gates for each operation mode of the shutdown cooling system. OM, operation mode.

diagram of the SCS is shown in Fig. 14. In the plant shutdown phase, there are five system configurations for the SCS [23].

- CONF1: Normal (Train A and B standby)
- CONF2: Train A operation (Train B standby)
- CONF3: Train B operation (Train A overhaul)
- CONF4: Train A operation (Train B overhaul)
- CONF5: Train B operation (Train A standby)

The fault tree shown in Fig. 15 is used to evaluate the unavailability of the SCS and a postprocessing method and condition gates [24] are commonly applied according to each system configuration. When both Train A and Train B are on standby, as the SCS becomes unavailable if both trains fail during standby status, the static AND gate is able to describe the relations between the failures of Train A and Train B. When one train is operating and the other train is being overhauled, as the SCS is unavailable if the operating train fails, the failure of the SCS can be modeled using the static AND gate adopting postprocessing methods or conditioning methods. However, when one train is operating and the other train is on standby, the failure of the SCS cannot be described accurately using the static AND relation between the failure of the operating train and the failure of the standby train. If the operating train fails, the standby train enters operating status and the failure rates of the components become higher compared to the standby status. As the standby train might fail either during standby status or operating status, the failure sequence of two trains and the state transition of the standby train should be considered. Therefore, a dynamic gate is necessary to exactly model the failure of the SCS during the CONF2 and CONF5, and the failure of substituting the failed train with the standby train should also be considered.

5.2. *Dynamic spare node combined with reliability matrix*

The dynamic fault trees [9,10] have some limitations to analyze the dynamic aspects in the failure of the SCS in the following areas. First, the dynamic fault tree does not provide a dynamic gate that is able to describe the redundancy concept explained in the previous section. The states of the components in the standby train change from the standby status to the operating status simultaneously when a problem arises in the operating train. As the spare gate of the dynamic fault tree accepts only the basic events as inputs, it cannot model the redundancy mechanism in which a train composed of various valves and pumps is on standby for the other train which is also composed of various components. Second, the backup components under the dynamic gate of the dynamic fault tree substitute for the main component if they do not fail before the failure of the main component. In other words, the failures of substituting a failed train that might be caused by human operators cannot be considered. Last, the dynamic fault tree does not provide a solution to simultaneously analyze the redundancy mechanisms and operation mode changes of the SCS.

In this section, how to apply the proposed dynamic RGGG to the reliability analysis of the SCS is explained. The reliability matrix is utilized to model various operation modes with one RGGG, and the dynamic spare node [11,12] is used to describe the redundancy mechanism of the SCS. Three operation modes of the SCS are assumed for simplicity.

- OM1: Both Train A and Train B are on standby.
- OM2: One train is operating and the other train is on standby.

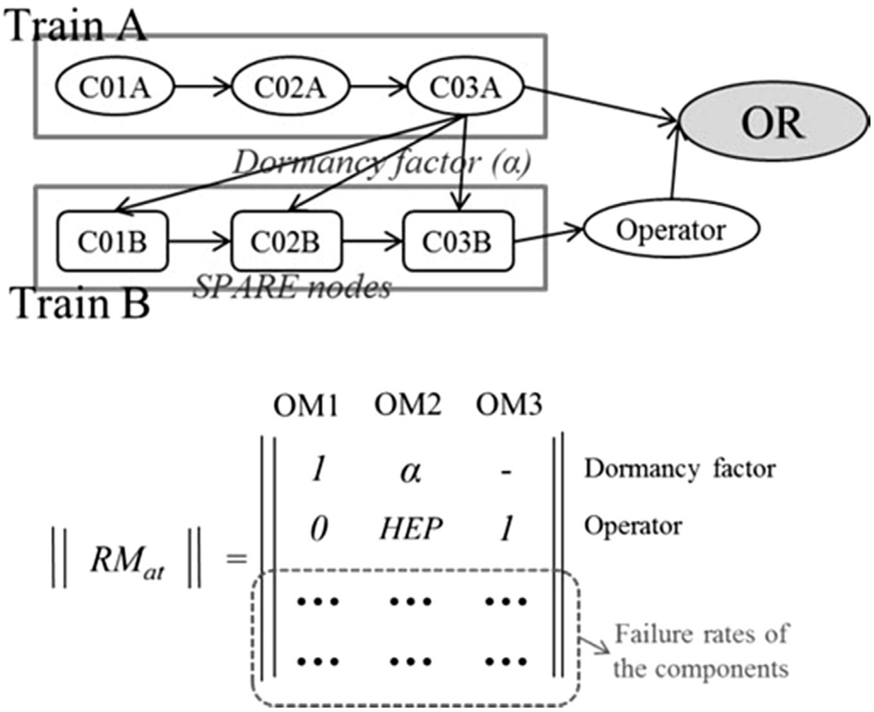
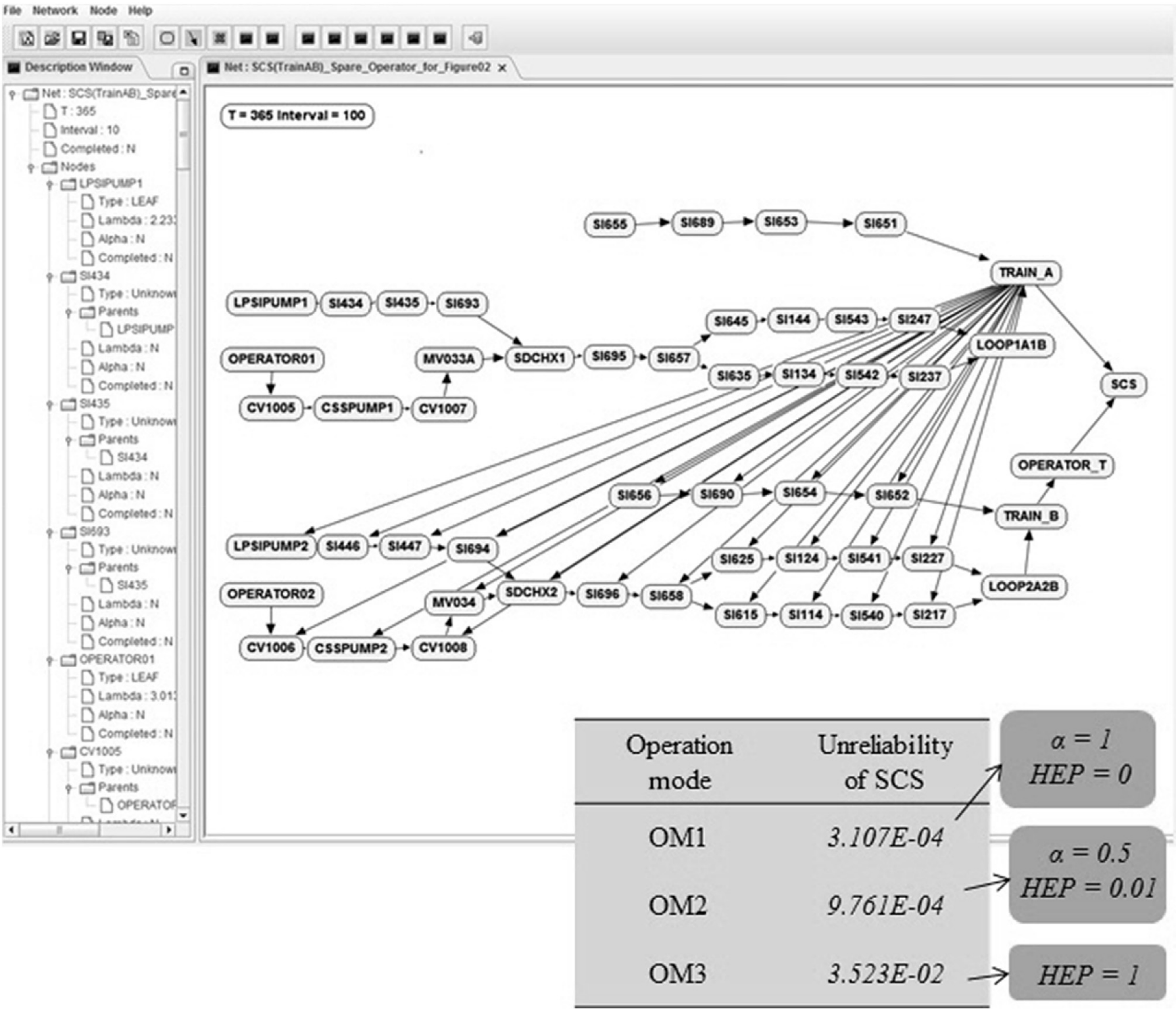


Fig. 18 – Simplified dynamic reliability graph with general gates with a reliability matrix for the shutdown cooling system. HEP, human error probability; OM, operation mode.

- OM3: One train is operating and the other train is unavailable due to an overhaul.

The dynamic spare node [11,12] has one primary input and spare inputs with a dormancy factor (α). It generates a failure output when the primary input and all the spare inputs fail. The dormancy factor is defined as the ratio of the failure rate in standby status to the failure rate in operating status. If the dormancy factor is 1, the failure rate in standby mode is equal to the failure rate in operational mode, and if the dormancy factor is zero, the corresponding component never fails in standby mode. The spare node is modified to express the dynamic redundancy mechanisms of the SCS in this study. The original spare node [11,12] and the modified spare node are shown in Fig. 16. The principle reason for modifying the original spare node is to conveniently model the dynamic relations that a problem in the operating train affects all the components in the standby train. The component modeled in the modified spare node n_2 in Fig. 16B becomes an operating status when there is no input signal from the main component (train) modeled in node n_1. The algorithm to make the probability table for the spare node [11,12] is also modified to be suitable for the modified spare node.

To analyze three operation modes using one RGGG model, a reliability matrix is used and the dormancy factor used in the spare nodes also varies according to the reliability matrix as the operation mode changes. Fig. 17 shows simplified RGGGs for each operation mode. The spare nodes with a dormancy factor are used to model OM2, while dynamic nodes are not necessary for OM1 and OM3. Three RGGGs in Fig. 17 can be integrated into one RGGG with a reliability matrix as shown in Fig. 18. The node of Operator is used to express the failure to substitute the failed train with the standby train. If the operator fails to substitute for the failed train of the SCS, the SCS loses the ability to remove the residual heat even though there is no fault in the standby train. The human error probability (HEP) represents the probability of a substitution failure and it is used to quantify the node of Operator. The first



Net : SCS(TrainAB)_Spare
T : 365
Interval : 10
Completed : N
Nodes
LPSIPUMP1
Type : LEAF
Lambda : 2.23
Alpha : N
Completed : N
SI434
Type : Unknow
Parents
LPSIPUMP
Lambda : N
Alpha : N
Completed : N
SI435
Type : Unknow
Parents
SI434
Lambda : N
Alpha : N
Completed : N
SI693
Type : Unknow
Parents
SI435
Lambda : N
Alpha : N
Completed : N
OPERATOR01
Type : LEAF
Lambda : 3.01
Alpha : N
Completed : N
CV1005
Type : Unknow
Parents
OPERATOF

Operation mode	Unreliability of SCS
OM1	3.107E-04
OM2	9.761E-04
OM3	3.523E-02

Fig. 19 – Dynamic reliability graph with general gates for the shutdown cooling system and estimation results. HEP, human error probability; OM, operation mode; SCS, shutdown cooling system.

and second rows of the reliability matrix in Fig. 18 respectively represent the dormancy factors and failure probability of the Operator node for each operation mode, and the other rows are for the failure rates of the subcomponents of the SCS. If the dormancy factor and HEP are set to 1 and 0, respectively, as shown in the reliability matrix, the RGGG in Fig. 18 becomes the same as the RGGG for OM1 in Fig. 17. If the HEP is set to 1, as Train B is never able to substitute for Train A, the RGGG in Fig. 18 becomes the same as the RGGG for OM3 in Fig. 17.

5.3. *Dynamic RGGG model for shutdown cooling system*

The shutdown cooling system shown in Fig. 14 can be modeled as a dynamic RGGG shown in Fig. 19. The spare nodes described above are used to model the redundancy mechanism during OM2. Using the reliability matrix to define changes of the failure rates, the dormancy factor, and HEP according to each operation mode, one dynamic RGGG model shown in Fig. 19 is able to include all the operation modes. The reliability of the SCS during OM1 estimated from the dynamic RGGG is the same as the estimation result from the static fault tree for OM1 shown in Fig. 20.

Table 11 compares the estimation results for OM 2 assuming no human error (HEP = 0) from the dynamic RGGG with those from the static fault tree as the dormancy factor changes. Since the static fault tree cannot consider the dynamic status changes of Train B from standby status to operating status, the estimation results become more inaccurate as the dormancy factor becomes smaller. That is because the smaller dormancy factor implies bigger differences between the failure rates of the components in Train B under standby status and operating status.

The dynamic RGGG model for the SCS has a very similar shape with the actual structure of the SCS shown in Fig. 14. Therefore, from the graphic display of the RGGG, it is very easy to see the system failure modes and ascertain the important events that cause a system failure and the effects of the events on the system reliability. For example, during OM2, the failure of substituting a failed train with a standby train might have a significant effect on the reliability of the SCS, and can be inferred easily from the RGGG model. The HEP for the train substitution can be reduced when there is a supervisor or an automated operator support system. To investigate the effect of the variation of substituting error probability on unreliability of the SCS, the probabilities of 0.01, 0.005, and 0.001 are

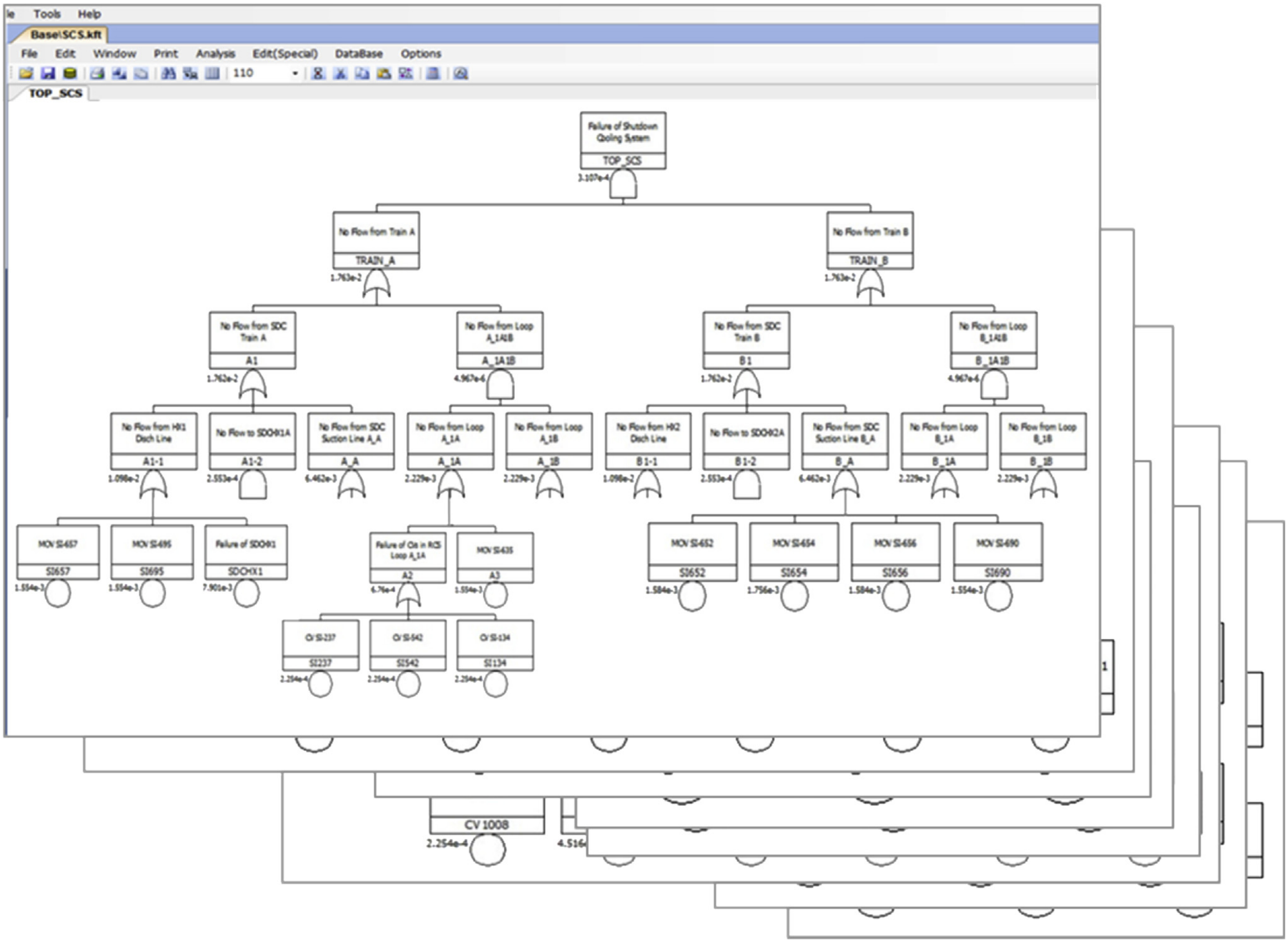


Fig. 20 – Static fault tree for the shutdown cooling system. SCS, shutdown cooling system; SDC, shutdown cooling.

selected representatively as the HEP and the estimation results are shown in Table 12.

6. Discussion

The fault tree analysis is the most widely used method in the risk assessment of nuclear power plants and for the modeling of the change of operation modes and failure criteria. The dynamic fault tree has been developed by adopting house events and a house events matrix. The dynamic fault tree provides magnificent ways to analyze the risk of dynamic systems, but since modeling fault trees for complex systems with complicated conditions is a very cumbersome task, it might cause errors in the construction of fault trees. Therefore, this study was conducted to propose a convenient modeling method for the reliability analyses of complex dynamic systems that have various operation modes varying with time. The RGGG method is improved because it is an advanced reliability graph model that was developed for the intuitive modeling of a target system from its functional block diagram and paves the way for the convenient reliability analysis of complex systems. To describe various operation modes varying with time by one RGGG, a novel concept of a reliability matrix is proposed with an explanation of how to utilize the reliability matrix in the RGGG for the various cases of configuration changes.

If a system has several operation modes and the system failure criterion changes during a certain process time, the number of conventional RGGGs required for the reliability analysis is the same as the number of operation modes. In addition, the probability tables used in the RGGG has to be modified according to the structure of the RGGG for the quantitative analyses. However, with the proposed reliability matrix, one RGGG is able to involve various conventional RGGGs. In addition, the replacement of the reliabilities of the components according to the reliability matrix has the same effect as changing the numerical expressions in the probability tables. Therefore, the probability tables of the nodes in the RGGG do not have to be modified as the system operation mode changes, and it could relieve difficulty in modeling various operation modes. Furthermore, the sequence-dependent failures and various change of operation modes can be analyzed at once using the dynamic nodes in combination with the reliability matrix. The reliability of an SCS which has various operation modes during the LPSD period can be analyzed using the proposed dynamic RGGG with dynamic nodes and reliability matrix. The dynamic redundancy mechanism which considers the substitution failure and various operation modes of the SCS can be analyzed with only one dynamic RGGG. In addition, as many kinds of logic between the events which have even multiple states can be modeled intuitively with one node in the RGGG method by defining the appropriate probability tables, the proposed method has wide applicability to various failure mechanisms, while a limited function such as OR and AND logics and binary states are provided in the fault tree analysis.

The RGGG method is an intuitive and convenient graphical modeling method especially for complex systems and by utilizing the reliability matrix, the dynamical system behavior and time-dependent system reliability also can be easily analyzed. However, the shortcoming of the RGGG method is that it is not able to produce minimal cut sets that describe the combinations of component failures that cause a system failure. As the minimal cut sets are important information for a system's safe operation and provide some insight into the system behavior, it is one of the most valuable outcomes of the fault tree analysis. That is, as each method has its own peculiar features and advantages, reliability analysis methods should be chosen or used together depending on the properties of the target system and the analysis purpose by taking account of each method's advantages.

Table 11 – Comparison of the estimation results between a dynamic reliability graph with general gates and a static fault tree (Operation Mode 2).

Dormancy factor	Unreliability of SCS	
	Dynamic RGGG	Static fault tree
$\alpha = 1$	1.241E−03	1.241E−03
$\alpha = 0.5$	6.318E−04	6.210E−04
$\alpha = 0.1$	1.437E−04	1.243E−04

RGGG, reliability graph with general gates; SCS, shutdown cooling system.

Table 12 – Unreliability changes according to the change of human error probability (Operation Mode 2).

HEP	Unreliability of SCS
0.01	9.761E−04
0.005	8.044E−04
0.001	6.664E−04

HEP, human error probability; SCS, shutdown cooling system.

Conflicts of interest

All authors have no conflicts of interest to declare.

Acknowledgments

This research was supported by a Nuclear Research & Development Program of the National Research Foundation (NRF) grant funded by the Korean government, Ministry of Science, ICT & Future Planning (Grant code: 2012M2B2B1055615).

REFERENCES

[1] US Nuclear Regulatory Commission (USNRC), Fault Tree Handbook, NUREG-0492, Washington (DC), 1981.

[2] US Nuclear Regulatory Commission (USNRC), PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300, Washington (DC), 1983.

[3] US Nuclear Regulatory Commission (USNRC), Traditional Probabilistic Risk Assessment Methods for Digital Systems, NUREG/CR-6962, Washington (DC), 2008.

[4] N.D.H. Desmond, B.B. Gregory, M.D. Karl, Risk and Uncertainty in Dam Safety, Thomas Telford Publishing, London, 2004.

[5] M.C. Kim, P.H. Seong, Reliability graph with general gates: an intuitive and practical method for system reliability analysis, Reliab. Eng. Syst. Saf. 78 (2002) 239–246.

[6] T. Matsuoka, M. Kobayashi, GO-FLOW: a new reliability analysis methodology, Nucl. Sci. Eng. 98 (1988) 64–78.

[7] T.S. Liu, S.B. Chiou, The application of Petri nets to failure analysis, Reliab. Eng. Syst. Saf. 57 (1997) 129–142.

[8] W.G. Schneeweiss, Tutorial: Petri nets as a graphical description medium for many reliability scenarios, IEEE Trans. Reliab. 50 (2001) 159–164.

[9] J.B. Dugan, S.J. Bavuso, M.A. Boyd, Dynamic fault-tree models for fault-tolerant computer systems, IEEE Trans. Reliab. 41 (1992) 363–377.

[10] M. Cepin, B. Mavko, A dynamic fault tree, Reliab. Eng. Syst. Saf. 75 (2002) 83–91.

[11] S.K. Shin, P.H. Seong, Adding dynamic nodes to RGGG and making probability tables, Trans. Am. Nucl. Soc. 97 (2007) 131–132.

[12] S.K. Shin, P.H. Seong, Review of various dynamic modeling methods and development of an intuitive modeling method for dynamic systems, Nucl. Eng. Technol. 40 (2008) 375–386.

[13] A. Kaufmann, D. Grouchko, R. Cruon, Mathematical Models for the Study of the Reliability of Systems, Academic Press, New York, 1997.

[14] R.A. Sahner, K.S. Trivedi, A. Puliafito, Performance and Reliability Analysis of Computer System: An Example-Based Approach using the SHARPE Software Package, Kluwer Academic Publishers, Dordrecht, 1995.

[15] A. Bobbio, L. Portinale, M. Minichino, E. Ciancamerla, Improving the analysis of dependable systems by mapping fault trees into Bayesian networks, Reliab. Eng. Syst. Saf. 71 (2001) 249–260.

[16] J.G.T. Toledano, L.E. Sucar, Bayesian networks for reliability analysis of complex systems, in: Proceedings of the 6th Ibero-American Conference on AI (IBERAMIA), Lisbon (Portugal), 1998.

[17] M.C. Kim, P.H. Seong, An analytic model for situation assessment of nuclear power plant operators based on Bayesian inference, Reliab. Eng. Syst. Saf. 91 (2006) 270–282.

[18] S.J. Lee, P.H. Seong, An analytical approach to quantitative effect estimation of operation advisory system based on human cognitive process using the Bayesian belief network, Reliab. Eng. Syst. Saf. 93 (2008) 567–577.

[19] S.K. Shin, P.H. Seong, A quantitative assessment method for safety–critical signal generation failures in nuclear power plants considering dynamic dependencies, Ann. Nucl. Energy 38 (2011) 269–278.

[20] International Electrotechnical Commission (IEC), Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, IEC 61508, Geneva, 1998.

[21] L. Lu, G. Lewis, Configuration determination for *k*-out-of-*n* partially redundant systems, Reliab. Eng. Syst. Saf. 93 (2008) 1594–1604.

[22] Microsoft Research, [Internet]. MSBNx (Microsoft Bayesian Network Editor) [cited 2015 Mar 5]. Available from: http://research.microsoft.com/en-us/um/redmond/groups/adapt/msbnx/.

[23] H.G. Kang, S.C. Jang, Fault-tree based risk assessment for dynamic condition changes, Nucl. Eng. Technol. 39 (2007) 139–144.

[24] H.G. Lim, J.H. Park, S.H. Han, S.C. Jang, Fault tree conditioning methods to trace system configuration changes for the application to low-power/shutdown PSA, Reliab. Eng. Syst. Saf. 94 (2009) 1666–1675.