FAULT-TREE-BASED RISK ASSESSMENT FOR DYNAMIC CONDITION CHANGES

HYUN GOOK KANG* and SEUNG-CHEOL JANG
Korea Atomic Energy Research Institute
150 Deokjin-dong, Yuseong-gu, Daejeon, 305-353 Korea
*Corresponding author. Email: hgkang@kaeri.re.kr

Received September 29, 2006
Accepted for Publication January 19, 2007

In order to apply a static fault-tree (FT) method to a system or a plant whose configuration changes dynamically, condition gates and a post processing method are used to effectively accommodate these changes. An operator's performance change, which can be caused by these configuration changes, should also be considered to assess the risk to a plant in a more realistic manner. This study aims to develop an integrated framework to accommodate various configuration changes and their effect on an operator's performance by using the FT model. We applied a condition-based human reliability assessment (CBHRA) method to consider various conditions endured by an operator. That is, we integrated the CBHRA method with the conventional post processing method for modeling the system configuration changes. The effect of the condition monitoring systems installed in a plant is also considered. In this study, we show an example application of the integrated framework to a probabilistic safety assessment for the shutdown phase of a nuclear power plant.

KEYWORDS : Fault Tree, System Analysis and Design, System Configuration Change

1. INTRODUCTION

For the past several decades, probabilistic safety assessment (PSA) techniques have been used to assess the relative effects of contributing events on system-level safety or reliability. They provide a unifying means of assessing physical faults, recovery processes, contributing effects, human actions, and other events that have a high degree of uncertainty. Among various modeling techniques, the fault tree (FT) is the most familiar to PSA staffs. And the FT's logical and simple structure makes it easy for design engineers to get useful information for system improvement.

The merits of the FT model, simplicity and easiness, come from its static nature. For the steady-state normal operation case, the FT effectively evaluates a risk. When the plant's condition changes, however, we have to develop a new model for reflecting the effect of the change. In order to reduce these repeated efforts, condition gates and a post processing method are commonly applied.

A plant operator tries to manipulate the plant to a safe state. A lack of necessary information, such as a loss of corresponding alarms and indications, will result in error-forcing contexts for an operator. In addition to supplying indispensable information, the monitoring systems installed in safety-critical plants provide more processed information to an operator. The operator's manipulation performance and his/her response to a plant abnormality will be affected by the availability of this information. The quantification of a human error probability (HEP) dominates the quality of a PSA, which plays a very important role in proving the safety of a system or a plant [1].

In this study, we apply the post-processing approach to accommodate this complicated situation by using the static FT. In section 2, we will briefly explain the condition -based human reliability assessment (CBHRA). In section 3, we will show an example application of the suggested framework to the shutdown cooling system of a Korean Standard Nuclear Power Plant.

2. CONDITION-BASED HUMAN RELIABILITY ASSESSMENT

In this section, we will briefly describe the concept of the CBHRA, which has been proposed by the authors elsewhere [1] and generalize the method to apply it to the plant configuration change modeling. In safety-critical systems, such as nuclear power plants, for the anticipated design basis accident, safety-critical mitigation systems are automatically actuated. In an emergency case, the human operator could also play the role of a backup for the

automated systems. That is, the failure of a safety feature actuation signal implies a concurrent failure of the automated systems and that of a manual actuation.

Quantification as part of a human reliability assessment involves the derivation of a probability distribution for a basic event modeled in the PSA. Each HEP consists of one unsafe action (UA) of which the probability is affected by the error forcing contexts (EFC). If the safety signal generation is automated, the probability of the human's omission error (UA) is the conditional upon the failure of the automated system. The safety signal generation failure could be caused by consecutive failures of automated systems and human operators. Given an accident scenario, the signal generation failure probability (F) has been formulated in a previous study [2] as:

$$F = \sum_i \sum_j P(UA \mid A_i, S_j) P(A_i \mid S_j) P(S_j) \qquad (1)$$

We have to consider two reasons for signal generation failure: automated system failure and manual actuation failure. The failures of sensors are independent from the accident scenario. For sensors and automatic systems, in consideration that the failure of an automatic system implies the failure of a safety signal generation and the loss of alarms, the signal generation failure probability can be calculated as in Equation (1). A_i and S_j denote the failure of the automated systems (excluding instrumentation sensors) and that of the sensors, respectively. This CBHRA method aims to evaluate the effects of an operator's performance change under a failure condition where computerized equipment automatically generates a reactor trip signal.

Briefly, Equation (1) considers two kinds of EFC: sensor failure and alarm failure. In order to develop a general framework of a post processing, we consider more kinds of EFC, including plant status information and component status information. The suggested framework also covers the case where automated signal generation equipment is not installed.

The plant status information includes the alarms and operation phase indications among which some are generated by the automatic system and failure of which is also a reason for a safety-signal generation failure. We assume that the monitoring system will provide component status information by an alarm.

For the example, assume a two-train safety-critical water supply system with a redundant means of supply. In the maintenance period (low-power and shutdown operation), one out of two trains might be unavailable due to a test and maintenance. If the operator correctly recognizes the plant operating state (POS), i.e., if he/she has information as to which train is unavailable, the probability that he/she manipulates the system in a right manner will increase. In the case of failure of normal components, if there is a monitoring system which notifies the operator about the status of the components, the success probability of the actuation of a redundant means will also increase.

In order to accommodate this situation, we generalized Equation (1) by using the assumption that there will be no interaction among the EFCs.

$$F = \sum_k P(UA \mid A, EFC_k) P(A \mid EFC_k) P(EFC_k) \qquad (2)$$

where the EFC_k stands for the *k*th condition of the EFCs. In the case that no automated signal generation equipment is installed, equation (2) can be simplified, as in equation (3).

$$F = \sum_k P(UA \mid EFC_k) P(EFC_k) \qquad (3)$$

The steps for an application of the proposed method are:

(1) Developing a set of conditions based on the investigation of possible EFCs and their effects on the operator performance
(2) Estimating the HEP for each condition
(3) Constructing a fault tree which includes a single human error (HE) event for each manual action
(4) Obtaining minimal cut sets (MCS) by solving the fault tree
(5) Post processing of the MCSs for a plant condition
(6) Post processing of the MCSs for a HEP determination

The purpose of step (1) is the development of the EFC groups. Since the consideration of all the EFC combinations in a separate manner is very complicated, we have to categorize possible EFC combinations into several groups in order to treat them in a practical manner. The post processing, which will be described in step (6), should be performed in consideration of the unavailable trains, unavailable components, and the effects of the monitoring systems.

Step (2) is the estimation of the HEP for each condition. If there is a monitoring mechanism which provides proper information to the operator, the corresponding EFC condition should imply a lower HEP value. On the contrary, in the case of a lack of information, the HEP will increase.

Steps (3) and (4) are for developing a fault tree model and getting the MCSs by using a PSA software package. In this phase, the developed fault tree will include a single HE event for each manual action.

Step (5) implies that if the plant has an unavailable safety train, its function should be disabled (equal to logic true) in the fault tree. The values of failure events of components in the train should also be 'true'.

In step (6), the probability of a HE event developed in step (3) will be replaced as a HEP estimated in step (2) in consideration of the component failures in each MCS. In

a set of MCSs, step (7) implies a substitution of the HE event with the EFC-group-specified HE event in consideration of the other events in each MCS. For example, the event of 'the manual reactor trip failure (MRTF)' should be substituted by one of the possible EFC-group-specified HE events: 'MRTF given EFC group 1', 'MRTF given EFC group 2', …, or 'MRTF given EFC group n'.

A manual implementation of steps (5) and (6) is expected to require much effort. Therefore, an automatic conditioning with a PSA software package is recommended. An automatic conditioning could be enabled based on logical rules, such as the following: 'if there are more than three sensor-failure events in the MCS, then substitute the basic HE event with the HE event given no alarm and no indication'; 'if there is no sensor failure, then substitute the basic HE event with the HE event given no alarm and all indications'; etc.

3. EXAMPLE APPLICATION

In order to prove the effects of the proposed framework, we apply the framework to a shutdown cooling system (SCS) in a nuclear power plant whose function is residual heat removal after a reactor shutdown. Figure 1 shows an overview of the SCS.

The example in this study does not include the automated signal generation equipment. For a case that automated signal generation equipment is installed, we show an example of an application in the authors' previous study [2]. In the example of this study, the operator has to manually initiate the SCS and manipulate pumps and valves in the SCS and also has to manually overcome various kinds of possible unavailability. Equation (3) will be applied to this example.

If this safety function of the SCS fails, then the coolant in the reactor vessel will boil and the nuclear fuel might be damaged. In order to meet the single failure criterion, the SCS consists of two trains. Each train has enough capability for cooling the residual heat. In normal cases, the low pressure safety injection (LPSI) pumps are used to supply the cooling water, but when the operator recognizes the failure of one LPSI pump path, he or she can re-establish the water path with the other LPSI pump. If there is no available redundancy in the LPSI pump, the operator can also re-establish the water path by using the containment spray system (CSS) pumps.

On the other hand, in the plant shutdown phase, there are 5 system configurations for the SCS. Sequentially, the following configurations will be applied to the SCS:
- CONF1 : Normal (Trains 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)

That is, there are two kinds of manual signal generations: a manipulation of the SCS to enter each system configuration (Action1) and a re-establishment of a water path from a LPSI pump to the other LPSI or CSS pump (Action 2).

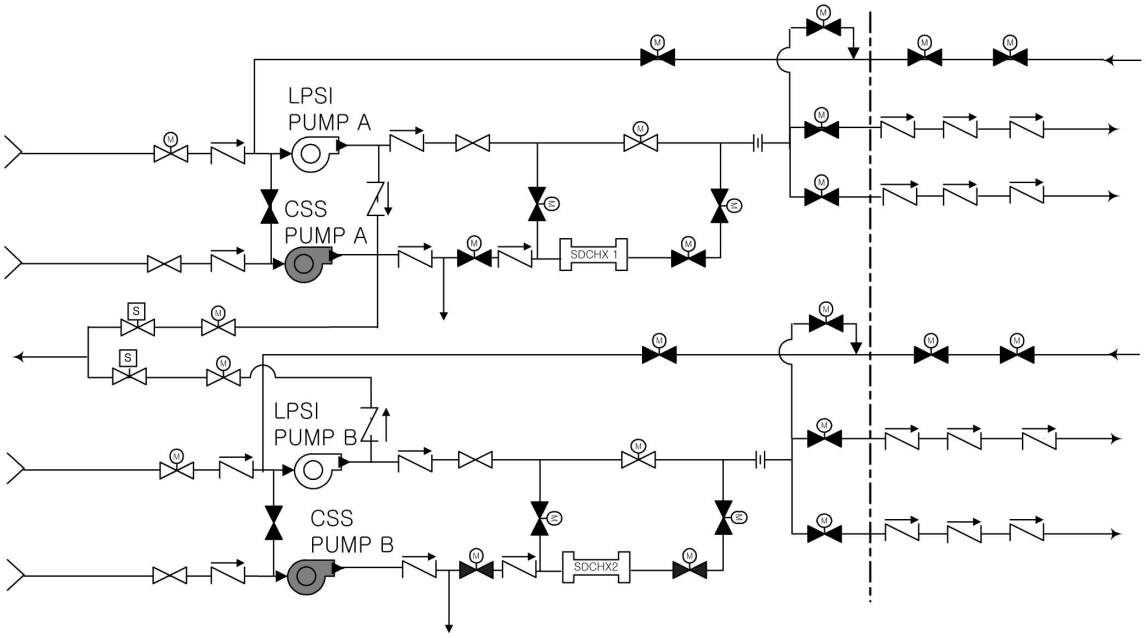

Fig. 1. Simplified Diagram for the Shutdown Cooling System (SCS) in a Typical Nuclear Power Plant [3]

Regarding step (1) of the suggested framework, the EFCs can be determined as:
- EFC1: Plant configuration
- EFC2: Failure of the components in the LPSI pump path

The EFC1 represents the stress that an operator faces when he/she should correctly recognize the current system configuration. The HEP can be improved to some extent when there is a supervisor or an automated operator support system (OSS). We consider only the OSS in this example. There are five configurations (CONF1 to CONF5), as mentioned above. In addition, there are two levels of support (no support case and OSS installed case). Regarding EFC1, we consider the 5x2 conditions.

The operator must recognize the status of a water path, which causes the EFC2. The HEP can also be improved if there is a monitoring system which provides information directly regarding the availability of the water path of the LPSI pump. The type and function of a specific unavailable component in each LPSI water path will affect the success probability of the water path change. However, in this example, we simply consider two cases: the successful recognition of the unavailability of the LPSI pump path and the recognition failure. In total, there are 10x2 EFC conditions.

For step (2), since the precise evaluation of the HEPs for each EFC condition is beyond the scope of this study, we used assumed values for HEPs. In the case of no OSS, the HEP of Action1 for the manipulation from the normal operation configuration to the single-train operation configuration (CONF1→CONF2) is assumed as 2E-3. The Action1 HEPs of other configuration changes of the single-train operation (→CONF3, →CONF4, and → CONF5) are also assumed to be 2E-3. The Action1 HEP of a configuration change from a single-train operation to a normal one (CONF5→CONF1) is assumed to be 1E-3. We assumed that if there is an OSS, the HEPs will be reduced to one tenth of the non-OSS cases. Table 1 summarizes the HEPs for Action1. The HEPs for Action2 are more complicated to estimate. Table 2 shows the assumptions made.

For steps (3) and (4), we developed a fault tree model of which the top logic is shown in Figure 2. Our model is modified from an established model for reflecting low-power shutdown conditions [4]. The fault tree was constructed and the MCSs were determined by using KIRAP [5], an integrated safety assessment software package developed at KAERI.

In step (5), we assigned a logical value of 'true' or 'false' for proper basic events to meet the following system configuration:
- CONF1: Components in Trains A and B are at standby
- CONF2: Components in Train A are in operation and those in Train B are at standby
- CONF3: Components in Train B are in operation and those in Train A are unavailable
- CONF4: Components in Train A are in operation and those in Train B are unavailable
- CONF5: Components in Train B are in operation and those in Train A are at standby

Table 1. The Assumed HEP for the Action 1 for Each EFC Condition

System Configuration Change	1→1		2→3		3→4		4→5		5→1	
OSS	O	X	O	X	O	X	O	X	O	X
LPSI Path Monitoring	Not applicable (No effect)									
Action1 HEP	2E-4	2E-3	2E-4	2E-3	2E-4	2E-3	2E-4	2E-3	1E-4	1E-3

Table 2. The Assumed HEP for the Action 2 for Each EFC Condition

System Configuration	1				2				3				4 (=3)				5 (=2)			
OSS	O		X		O		X		O		X		O		X		O		X	
LPSI Path Monitoring	O	X	O	X	O	X	O	X	O	X	O	X	O	X	O	X	O	X	O	X
Action2 HEP	IE-3	1E-2	2E-3	2E-2	2E-3	2E-2	4E-3	4E-2	1E-2	1E-1	2E-2	1E-2	1E-2	1E-1	2E-2	2E-1	2E-3	2E-2	4E-3	4E-2

For step (6), we apply the HEPs in Tables 1 and 2 in consideration of the system configuration. In order to observe the changes in the quantification result, the unavailability of the SCS under CONF1 and that under CONF3 are compared in Table 3. The effect of a HEP change is dominant in CONF1 since both trains are in the standby condition. The best system unavailability is 2.54E-3. The worst result of CONF1 shows an additional unavailability of 1.82E-3, which corresponds to 72% of the best result. However, in CONF3, since one train is unavailable and the component failure probabilities are dominant, the unavailability of SCS is less sensitive to the change of the HEPs. The worst case of CONF3 shows a 9% difference from the best case.

Table 3. The SCS Unavailability for Each EFC Condition

System Configuration	1				3			
OSS	O		X		O		X	
LPSI Path Monitoring	O	X	O	X	O	X	O	X
Action1 HEP	2E-4		2E-3		2E-4		2E-3	
Action2 HEP	1E-3	1E-2	2E-3	2E-2	1E-2	1E-1	2E-2	2E-1
SCS Unavailability	2.54E-3	2.55E-3	4.35E-3	4.36E-3	4.41E-2	4.50E-2	4.60E-2	4.79E-2

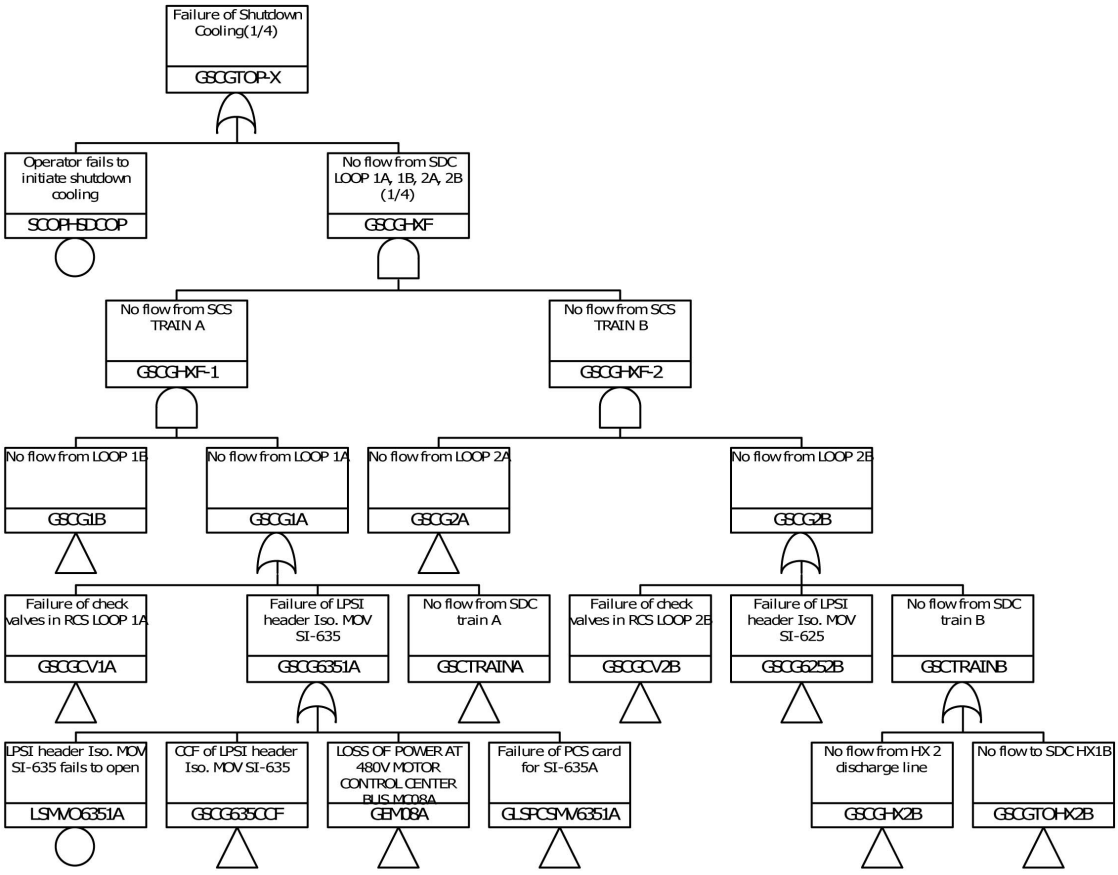

Fig. 2. The Top Logic of a Fault Tree Model for the SCS Failure

4. CONCLUSIONS

The quantification of a HEP dominates the quality of a PSA. In this study, we generalized the proposed CBHRA method and extended its applicability by integrating the post-processing methods for the operator's EFC. This framework provides an integrated means to accommodate the dynamic condition changes, the plant configuration changes, and the effects of these changes on a human operator by using the FT model.

The proposed framework aims to model the dynamic change of the plant and component conditions in a more systematic manner to overcome the demerits of the static FT. Especially, an improvement of the operator's performance due to the component monitoring systems and the automated operator support systems could be effectively modeled by using the FT based on the proposed framework.

We have presented an example application of the developed method to dynamic configuration changes of a system during a low-power shutdown phase of a nuclear power plant. The quantification results demonstrate the effectiveness of the proposed framework.

ACKNOWLEDGEMENT

This work has been carried out under the Nuclear R&D Program supported by The Ministry of Science and Technology, Korea.

REFERENCES

[1] Jung, W., Yoon, W.C., Kim, J.W., Structured Information Analysis for Human Reliability Analysis of Emergency Tasks in NPPs, Reliability Engineering and System Safety, Vol.71, No.1, p21-32, 2001.

[2] Hyun Gook Kang and Seung-Cheol Jang, "Application of Condition-Based HRA Method for a Manual Actuation of the Safety Features in a Nuclear Power Plant," *Reliability Engineering and System Science*, Volume 91, No. 6, p627-633, 2006.

[3] T. Seong, et al., *Low-Power Shutdown Probabilistic Safety Assessment for Yonggwang Unit 5&6*, ISA Team Technical Memo, KAERI, 2000.

[4] Ho-Gon Lim, Jin-Hee Park and Seung-Cheol Jang, Construction of a Shutdown PSA Model by Using a Full Power PSA Model, *KJPSA2006*, Cheju, November, 2006

[5] S.H. Han, et al., *User's Manual for KIRAP (KAERI Integrated Reliability Analysis code Package) Release 2.0*, KAERI/TR -361/93, 1993.