KAERI/TR-2907/2005

디지털 특성을 반영한 조건기반 인간신뢰도분석 방법론 연구

Condition-based Human Reliability Assessment for Digitalized Control Room

2005. 4

한 국 원 자 력 연 구 소

제 출 문

한국원자력연구소장 귀하

본 보고서를 2005년도 “정지/저출력 및 디지털 계통의 위험도 평가기술 개발” 과제의 기술보고서로 제출합니다.

2005. 4.

주 저 자 : 강현국 (종합안전평가부)

공 저 자 : 엄흥섭 (종합안전평가부)

장승철 (종합안전평가부)

하재주 (종합안전평가부)

요 약 문

인적 오류(Human Error)의 확률론적 추정은 원자력발전소 전체의 확률론적 안전성 평가 (Probabilistic Safety Assessment; PSA)에 매우 큰 영향을 미친다. 한편 최근 국내 표준원전에 도입되고 있는 디지털 안전계통은 디지털 기술의 특성상 다중의 기능을 동시에 수행하게 되므로 디지털 안전계통의 고장이 인적오류에 영향을 미쳐 궁극적으로 플랜트 전체의 안전성에 영향을 미칠 수 있으므로 이에 대한 상세 분석이 필요하다. 기존의 고장수목을 이용한 PSA 모델에서는 사고상황에서도 운전원에게는 모든 정보가 정상적으로 전달되는 것을 가정하여 단일사건으로 인적 오류를 취급하였으나, 보다 정확한 분석을 위해서는 이러한 상세분석을 바탕으로 현실적인 모델을 개발할 필요가 있다.

본 연구에서는 이러한 고장의 파급과 인적 오류 증가의 가능성을 정량적으로 평가하고 고장수목 모델에 반영하기 위한 방법론을 제시하였다. 먼저 해석적인 방법으로 기존의 단일조건 단일사건 모델의 타당성을 검토하였다. 검토결과 기존의 방법은 다중변수 안전기능에서는 비교적 근사적인 분석이 가능하나, 단일변수 안전기능의 경우에는 분석결과가 큰 차이를 보이는 것을 확인하였다.

따라서 본 연구에서는 '조건부 인적 오류 정량화(CBHRA)' 방법을 개발하였다. 인간 운전원이 당면하는 모든 상황에 대해 조건을 정하여 분석하는 것이 가장 정확한 분석방법이긴 하나 실제로 적용하기에는 큰 어려움이 있으므로, 이러한 상황을 디지털계통의 고장과 센서의 고장 등을 고려하여 몇개의 그룹으로 간략화하여 인적오류 확률을 산정한 후, 그 값을 기존의 단일 인적오류 사건 고장수목에 반영시키는 방법론을 제시하였다.

이렇게 개발된 CBHRA 방법론을 한국형 표준원전에 적용한 결과를 통해 이 방법의 유효성과 타당성을 검증하였다.

Summary

In safety-critical systems, the generation failure of an actuation signal is caused by the concurrent failures of the automated systems and an operator action. These two sources of safety signals are complicatedly correlated. The failures of sensors or automated systems will cause a lack of necessary information for a human operator and result in error-forcing contexts such as the loss of corresponding alarms and indications.

In the conventional analysis, the human error probabilities (HEP) are estimated based on the assumption of ‘normal condition of indications and alarms’. In order to construct a more realistic signal-generation failure model, we have to consider more complicated conditions in a more realistic manner. In this study, we performed two kinds of investigation for addressing this issue.

We performed the analytic calculations for estimating the effect of sensors failures on the system unavailability and plant risk. For the single-parameter safety signals, the analysis result reveals that the quantification of the HEP should be performed by focusing on the ‘no alarm from the automatic system and corresponding indications unavailable’ situation.

This study also proposes a condition-based human reliability assessment (CBHRA) method in order to address these complicated conditions in a practical way. We apply the CBHRA method to the manual actuation of the safety features such as a reactor trip and auxiliary feedwater actuation in Korean Standard Nuclear Power Plants.

In the case of conventional single HEP method, it is very hard to consider the multiple HE conditions. The merit of CBHRA is clearly shown in the application to the AFAS generation where no dominating HE condition exits. In this case, even if the HE conditions are carefully investigated, the single HEP method cannot accommodate the multiple conditions in a fault tree. On the other hand, the application result of the reactor trip in SLOCA shows that if there is a dominating condition, the use of single HEP method could be a practical way of developing a model.

Table of Contents

List of Tables

List of Figures

1. Introduction

In safety-critical systems such as in nuclear power plants, the safety-feature actuation is fully automated. 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 generation implies the concurrent failure of the automated systems and that of a manual actuation. Safety-critical parameters are instrumented by redundant sensors, and the conventional analog-circuit-based signal processing systems provide a fully redundant path for each sensor. Each of the redundant signal processing systems provides a corresponding alarm for an operator's easy recognition of the plant status.

It is widely recognized that sophisticated probabilistic safety assessment (PSA) techniques are critical in estimating the frequency of accidents in complex engineered systems such as nuclear power plant, aviation, aerospace, and chemical processing plant. It has been used to assess the relative effects of contributing events on system-level safety or reliability. The approach used in PSA is to model the system in terms of its components, stopping where substantial amounts of data are available for all of the key components.

PSA is increasingly being used as part of the decision making process to assess the level of safety of nuclear power plants. The accuracy of the result depends on the accuracy of the PSA model itself, and it has improved over time. The methodologies in use are maturing and the insights gained from the PSAs are being used along with those

from deterministic analysis.

In recent years many nuclear power plants have adopted modern digital I&C technologies since they are expected to significantly improve their performance and safety. By the general progress of I&C technologies for process engineering such as computer technology, control engineering, data processing and transfer technology, and software technology, the modern digital technologies were expected to significantly improve both the economical efficiency and the safety of nuclear power plants. The economical efficiency improvement due to digital applications seems clear, but the safety improvement is not well accepted. Even though the use of digital equipment for safety-related functions provides many advantageous features, there are still many arguable safety issues remained.

The Korean Standard Nuclear Power Plants (KSNPP), typically Ulchin 5 & 6 nuclear units, have adopted safety-critical digital systems such as a Digital Plant Protection System (DPPS) and a Digital Engineered Safety Feature Actuation System (DESFAS), due to the functional advantages of smart digital systems and the obsolescence of the traditional analog components. Thanks to the multi-tasking feature of digital systems, the safety-critical signal generation systems could also supply the alarms and key information to the human operator.

There are many issues due to the application of digital equipment to the safety critical systems such as nuclear plants. Followings are the characteristics of digital

systems from the PSA viewpoint.

i) The utilization of hardware is determined by software and inputs.

ii) The system could be multi-purpose.

iii) The failure modes are not well defined.

iv) Software might hide the transient faults of hardware.

v) Software fails whenever it executes the faulty part of code.

vi) The more efforts on the management of software quality could cause the lower expectation of software failure in operation phase, but its quantification is .

vii) Various monitoring and recovery mechanism can be adopted, but their coverage is not well defined.

viii) Apparently different components might cause common cause failure (CCF) because electronic components consist of a lot of small modules, which are manufactured in globally standardized environment.

ix) Digital systems are more sensitive to the environmental condition such as ambient temperature than conventional analog systems.

x) There might be no warning or insufficient information to operators when an automated system fails.

xi) The system failure might cause the blockage of safety-critical information from field to operators.

xii) New initiating events are possibly induced by digital system failure.

Many of the assumptions for quantitative analysis of a digital system are intentionally induced for the analysis simplicity, but some of them are due to failing to

give enough caution. Unreasonable assumptions result in unreasonable safety evaluation. The fault-free software or the perfect coverage of fault tolerance mechanism is a typical example.

This study addresses the issues of ii) and x). In other words, the use of digital systems for the safety-critical signal generation will affect the human operator's performance. The analysis of human performance becomes more complicated. Especially in the case of the KSNPP, several different functions such as an alarm generation, trip signal generation, and a safety-function-actuation signal generation for all the trip parameters are simultaneously performed by the DPPS. Therefore, in the event that the DPPS fails, an operator will not receive alarms related to the reactor trip and the automatic safety-feature actuation.

A human operator or a digital system generates safety-actuation signals, i.e., they are a part of the signal generation mechanism. Therefore, in order to assess their safety, we should consider the safety-function failure mechanism first. The reasons for a specific safety function failure can be categorized into two groups: the mechanical actuators' failure and the signal generation failure. The reason for a signal generation failure consists of two events: Automatic signal-generation failure and manual signal-generation failure. The human operator's manual action plays the role of a backup for the automatic signal generation.

With a consideration of these relationships, the reasons for a specific safety

function failure can be expressed as shown in Figure 1. Since a human operator or an automatic system generates safety-actuation signals, a signal generation failure implies the human operator's interception of an automatically generated signal or the concurrent occurrence of an automatic signal-generation failure and a manual signal-generation failure.

If an automatic system successfully generates the safety signals, a human operator does not have to generate the signal. That is, the human error probability (HEP) of a manual signal generation is a conditional probability given that the automatic signal generation fails. It is a kind of error of omission (EOO). The reason for an automatic generation failure could be the failure of the processing systems or that of the instrumentation sensors. A processing system failure deteriorates the performance of a human operator since it implies that the alarms from the processing system will not be provided to the operator. It is also obvious that the failure of the multiple redundant sensors also deteriorates the human performance since it will concurrently cause the loss of the corresponding sensor indications and the failure of automated signal-generation system which causes the loss of the corresponding alarms.

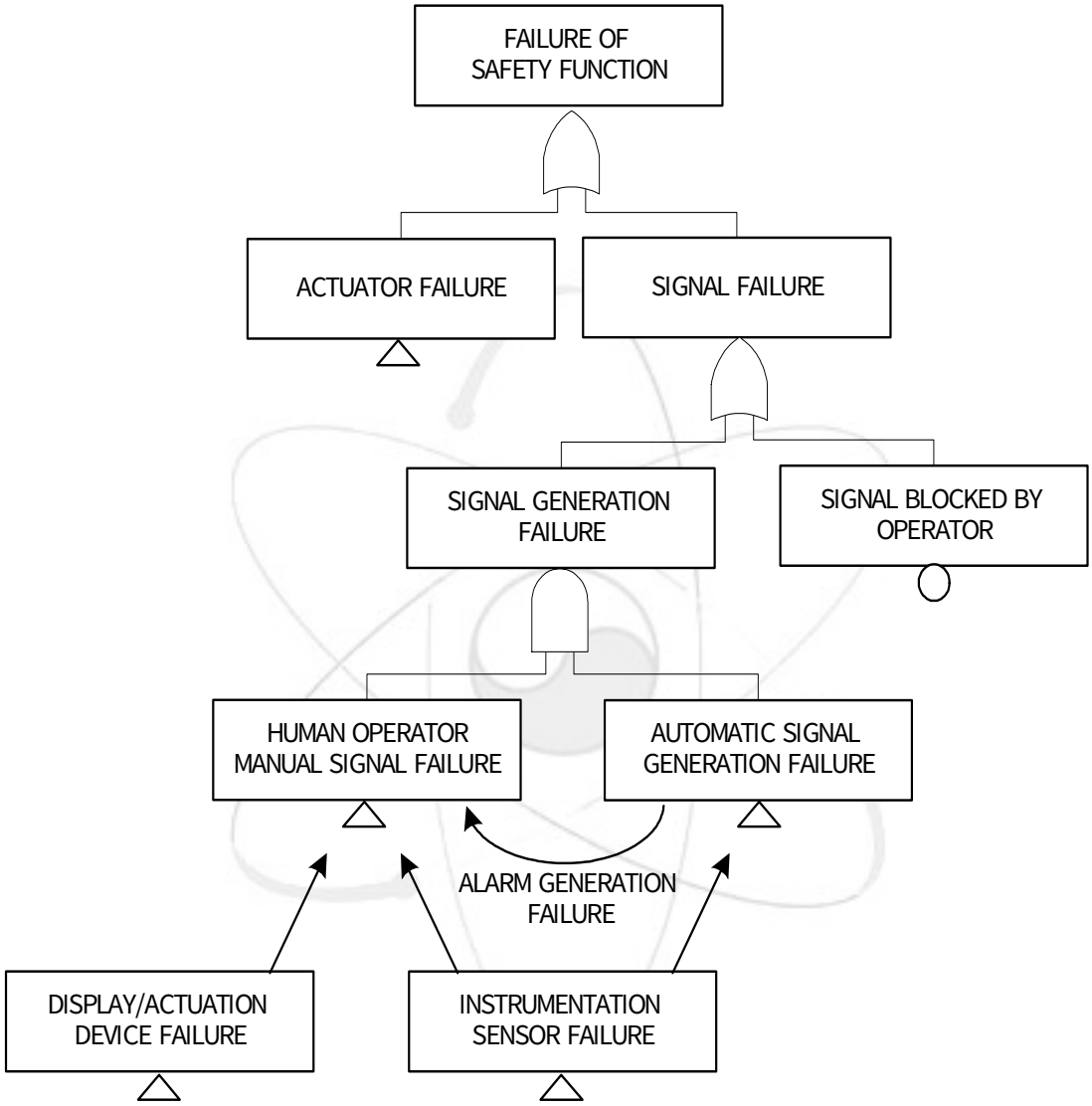

Figure 1. The schematic of the concept of the safety function failure mechanism

On the other hand, as shown in Figure 1, the operator may turn off the automatically generated signal based on a wrong decision. It is a kind of error of commission (EOC). The probability of this EOC is the conditional probability given that the automatic system successfully generates a proper signal using the sound sensors.

The methods of probabilistic safety assessment were broadly used not only for demonstration of plant operation risk level, but for many other applications connected with plant technology modifications, optimalization of technical specifications of plant operation, improvements of conditions of plant-staff work, development of continuously working risk monitor and a number of others. The quantification of a HEP dominates the quality of a PSA which plays a very important role in proving the safety of a system or a plant [1],[2].

Human reliability analysis (HRA) is performed as of nuclear power plant PSAs to produce probability estimates for human error events. In determining HEPs, most HRA methods account for the contextual aspects that contribute to human failure through the acknowledgment of plant conditions and performance-shaping factors (PSFs) potentially present during a task execution.

The process used in most HRA methods to estimate an HEP for a task of interest is to first, estimate the base HEP (referred to as a nominal or conditional probability by some methods); second, to define the set of PSFs that affect that task; and third, to identify the significance (i.e. the size of the effect) of each PSF and to combine

the effects of these PSFs to modify the base HEP for that task. Such a procedure is employed in many methods such as THERP.

A Technique for Human Event Analysis (ATHEANA) is a HRA method that was developed by the US Nuclear Regulatory Commission (USNRC) to increase the degree to which an HRA can represent the kinds of human behaviors seen in accidents and near-miss events at nuclear power plants and at facilities in other industries that involve broadly similar kinds of human/system interactions. The method provides a detailed search process for identifying important human actions and the contexts that can lead to their success or failure [3]. While ATHEANA provides guidance for quantifying human actions for PSA purposes, the final steps of the quantification process suggest that analysts translate the important contextual information identified with the search process into HEPs using existing HRA methods such as THERP.

Human reliability analysis has been understood to be one of key components of PSA effort. In the conventional PSA model of the KSNPP which consists of numerous event trees and fault trees, the failure of a signal generation which includes the event of human operator failures is modeled in the fault trees with a few basic events.

In the chapter 2, we will quantitatively explain the effect of the sensor failures on the manual operation failure based on analytic approach. In this study, we focus on the analysis of the manual signal generation failure. The HEP is affected by many information sources. In this paper, we only consider two information sources: Alarms and process-parameter indications. For simplicity, the failure of display systems is not considered. As a typical example, we illustrate its application to the safety-signal

generation in the case of digital automated signal generation systems, the DPPS and the DESFAS. We consider two kinds of safety signals in the DPPS and the DESFAS: Reactor trip signal and engineered-safety-feature (ESF) actuation signals.

In order to construct a more realistic signal-generation failure model, we have to consider more complicated conditions in a more realistic manner. The chapter 3 aims at suggesting the modeling method of conditional HEPs with the condition-based human reliability assessment (CBHRA). The CBHRA method enables the treatment of complicated conditions in a practical way with familiar fault tree models. This chapter also demonstrates the usefulness of the CBHRA method based on the example application to the DPPS and the DESFAS in the KSNPP.

2. Analytic Calculation of Safety Function Failure Probabilities

In consideration of sensors, automatic systems and operators, if they are assumed to be independent, the probability of the safety-actuation signal generation failure, F, could be defined as

$$F = \sum_i \sum_j P(H \mid A_i, S_j) P(A_i) P(S_j) \tag{1}$$

where H : the human operator failure,

A_i : the status of an automatic system (A_0: normal and A_1: failure), and

S_j : the status of instrumentation sensors (j = 0, 1, 2, … , n).

In real cases, the combined failures of sensors and automatic systems in redundant channels contribute to F to some extent. In safety-critical systems such as nuclear power plants, however, we could roughly assume as in Equation (1) since the common cause failures of redundant channels are dominant contributors to F.

In the case that the instrumentation channel provides enough information for automatic signal generation, if we ignore the EOC of the operator, we could consider $P(H \mid A_0, S_j)$ equals zero because A_0 implies that the automatic system successfully generates the target signals (trip and alarm signals). In the other case, even though the automatic system operates normally, there will be no automatic signal generation.

2.1 Single-Parameter Safety Function

Assume a typical single-parameter ESF signal which is activated by four redundant sensors based on 2-out-of-4 logic. If S_j could be defined as in Table 1, for j = 0 to 10, there will be an automatic signal generation and $P(H \mid A_0, S_j) = 0$. For j = 11 to 15, we don't have to consider the status of the automatic system because no sensor initiates the target ESF signal or the corresponding alarm. That is, for j = 11 to 15, $\sum_{i=0}^{1} P(H \mid A_i, S_j) P(A_i) = P(H \mid S_j)$. From Equation (1), F could be expressed as

$$F = P(A_1) \sum_{j=0}^{10} P(H \mid A_1, S_j) P(S_j) + \sum_{j=11}^{15} P(H \mid S_j) P(S_j). \qquad (2)$$

For j = 0 to 4, $P(H \mid A_1, S_j)$ implies the probability that the human operator fails to manually actuate the ESF signal where three or more indications are available and no alarm is available. For simplicity, we assume that three or four correct indications out of total four indications could deliver similarly clear information to the operator. We define $P(H \mid A_1, S_j) = P_{H0}$ for j = 0 to 4. On the other hand, for j = 5 to 15, $P(H \mid S_j)$ implies the probability that the operator fails to actuate the signal where two or less correct indications out of four and no alarm is available. We define $P(H \mid S_j) = P_{H1}$ for j = 5 to 15. And for the simple notation, $P(A_1) = P_A$.

Table 1. The status of the instrumentation sensors

	Sensor A	Sensor B	Sensor C	Sensor D
S_0				
S_1	*FAIL*			
S_2		*FAIL*		
S_3			*FAIL*	
S_4				*FAIL*
S_5	*FAIL*	*FAIL*		
S_6	*FAIL*		*FAIL*	
S_7	*FAIL*			*FAIL*
S_8		*FAIL*	*FAIL*	
S_9		*FAIL*		*FAIL*
S_{10}			*FAIL*	*FAIL*
S_{11}	*FAIL*	*FAIL*	*FAIL*	
S_{12}	*FAIL*	*FAIL*		*FAIL*
S_{13}	*FAIL*		*FAIL*	*FAIL*
S_{14}		*FAIL*	*FAIL*	*FAIL*
S_{15}	*FAIL*	*FAIL*	*FAIL*	*FAIL*

In order to examine the effect of the sensor failure probability to the signal generation failure probability, we apply the Multiple-Greek Letter (MGL) method for estimating the common cause failure of sensors. The MGL method is one of the most popular methodologies in dealing with the multiple failures of identical sensors due to a common cause. For j = 1 to 4, $P(S_j)$ implies a sensor's independent failure probability. Based on NUREG/CR-4780 (Mosleh, 1988), $P(S_j) = (1-\beta)P_S$, where PS is the failure probability of each sensor. For j = 5 to 10, $P(S_j) = \beta(1-\gamma)\frac{P_S}{3}$. For j = 11 to 14, $P(S_j) = \beta\gamma(1-\delta)\frac{P_S}{3}$. And $P(S_{15}) = \beta\gamma\delta P_S$.

From Equation (2) and the above assumptions, an expression for the failure probability of an ESF signal which is generated by one parameter with four redundant identical sensors is derived as

$$F = P_{H0}P_A\{1+4(1-\beta)P_S\} + P_{H1}\{\frac{6}{3}P_A\beta(1-\gamma) + \frac{4}{3}\beta\gamma(1-\delta) + \beta\gamma\delta\}P_S . \qquad (3)$$

For illustrating the coefficients of HEPs, P_{H0} and P_{H1}, quantitatively, assume P_A and P_S as 10^{-6} and 10^{-2}, which are practical values in the case of a KSNPP [4], [5]. And β, γ and δ are assumed as 0.05, 0.5 and 0.9 respectively. Then, the coefficient of P_{H0} is 1.04E-6 (= 1.0E-6 + 3.8E-8) and that of P_{H1} is 2.58E-4 (= 5.0E-10 + 3.3E-5 + 2.3E-4) which is several hundred times larger. It is notable that 10^{-2} is selected for P_S based on the assumption that the sensor failures are undetectable within one-year maintenance period. If the sensor failure could be detected with more than 99%

probability, then P_{H0} and P_{H1} will have similar importance.

Conventionally the HEP is estimated based on the assumption that all the instrumentation and alarms deliver the information normally. However, this analysis result reveals that the quantification of the HEP should be performed by focusing on the 'no alarm from the DPPS and the corresponding indications unavailable' situation denoted by P_{H1} in this study. It is obvious that P_{H1} is much higher than P_{H0}. Therefore the main contributor to the failure of a safety signal is the last term. If the automatic signal generation system such as the DPPS/DESFAS is very unreliable (worse than the failure probability of 10^{-4}), the first term will be significant.

If we build an analysis model using fault trees, it is very hard to reflect two or more different cases of HEPs because of the static characteristic of the fault tree. In some cases, in order to get a more precise estimation of F, the HEP value should be modified in the process of the cutest analysis. It is a kind of the consideration of dependency between the HEPs, the status of sensors, and the status of automatic systems.

2.2 Multiple-Parameter Safety Function

For the multiple-parameter safety functions such as the reactor trip and the main steam line isolation, the probability of the safety-actuation signal generation failure could be redefined as

$$F = \sum_i \sum_j \{P(H \mid A_i, S_j^1, S_j^2, ..., S_j^n) P(A_i) \prod_k P(S_j^k)\}, \quad (4)$$

where S_k denotes the status of the sensors for the kth parameter and n denotes the number of parameters.

In the case of automatic systems available, if two or more sensors of one of multiple parameters exceed the preset value, the safety signal will be automatically generated and $P(H \mid A_0, S_j^1, S_j^2, ..., S_j^n) = 0$. Therefore the remaining cases are those one or no sensor is available for every parameter. As shown in the previous section, the probability of three failed sensors (3.3E-5) is relatively smaller than that of all-sensor failure (2.3E-4). For simplicity, in the case of automatic systems available, we consider only one case that all the sensors fail to deliver information. Then, the HEP is not affected by the status of the DPPS/DESFAS because the alarms from the DPPS/DESFAS and all the corresponding indications are not available to the operator.

In the case that the automatic systems are unavailable, $P(H \mid A_1, S_j^1, S_j^2, ..., S_j^n)$ and $\prod_k P(S_j^k)$ vary along the sensor status j. And there is no alarm available but some indications are available. In the redundant sensors' cases, the detailed calculation for

each S_j is impractical since the number of sensor status is R^n, where R denotes the number of sensor redundancies. The variation of $\prod_k P(S_j^k)$ is expected to be much larger than that of $P(H \mid A_1, S_j^1, S_j^2, ..., S_j^n)$ because the former varies from 10^{-9} to 1.0. For simplicity, we consider only one case that all the sensors successfully deliver correct information ($\prod_k P(S_0^k) \approx 1$).

With the above two rough assumptions, Equation (4) could be simplified as

$$F \approx P(H \mid \text{No sensor available}) \prod_{k=1}^{n} \beta^k \gamma^k \delta^k P_S^k + P(H \mid A_1, \text{All sensors available}) P_A \quad (5)$$

For an illustration, assume the example of a reactor trip signal when small LOCA accident happens. There are four parameters for the small LOCA [6]. For these four kinds of sensors, we simply assume the same PS and the same MGL parameters as in the previous section. The calculated coefficient of $P(H \mid \text{No sensor available})$ is 2.56E-15 and that of $P(H \mid A_1, \text{All sensors available})$ is 1E-6. Even though the HEP of the former case is obviously higher than that of the latter, the big difference between the coefficients results in a much higher contribution of $P(H \mid A_1, \text{All sensors available})$ to F.

It implies that the conventional assumption for the HEP is partly appropriate in the analysis of multiple-parameter safety signal failure. That is, in this case, the sensors provide correct information but the alarms from the DPPS/DESFAS are not available.

2.3 Plant Risk Effect Analysis

We performed a sensitivity study to demonstrate the effect of the HEPs. The Risk Monitor, a fault-tree model for the KSNPP developed by the Integrated Safety Assessment team at KAERI, is used to model the general plant risk of the KSNPP. It consists of about 2500 basic events and 3500 logical gates.

There are many HEPs in various manual actions in the Risk Monitor. Although they are fairly correlated, for simplicity, we do not consider the dependency among the HEPs. The selected variables are the HEPs for the safety signal generation of the single-parameter function. Considered safety signals are limited to the reactor trip signal and the ESF actuation signals. The HEPs for the multiple-parameter function are assumed to be the same as in the conventional analysis. It should be noted that it is optimistic assumption.

The reactor trip signal, safety injection actuation signal (SIAS), containment isolation actuation signal (CIAS) and main steam isolation signal (MSIS) are the multiple-parameter safety signals. Containment spray actuation signal (CSAS), recirculation actuation signal (RAS) and auxiliary feedwater actuation Signal–1 & 2 (AFAS-1 and AFAS-2) are the single-parameter safety signals. For the multiple-parameter signals, we use the same values as those in the conventional analysis [5], [7].

In order to demonstrate the difference from the conventional analysis results, we use different values for the single-parameter signals. We roughly assume that the operator will use a half of the given diagnosis time for estimating the parameter

corresponding to the failure sensors. And we also assume one more case that the operator spends two third of the diagnosis time for this estimation. Based on the conventionally estimated values and the HEP-diagnosis curve in the THERP methodology [8], we estimate the HEPs for the single-parameter signals. The detailed explanation for this assumption will be presented in chapter 3. The core damage frequency (CDF) of the KSNPP unit is used as the measure of the plant safety.

The conventional HEPs, the estimated HEPs and the corresponding CDF calculation results are shown in Table 2. The increases of the HEPs in the four single-parameter ESF signals cause about 3% and 7% increase of the plant CDF respectively. Figure 2 illustrates the changes in the CDF along with the HEP changes.

Table 2. The HEPs for the safety-signal generation and the CDFs.

	The HEP in conventional analysis	The HEP estimated (time: 1/2)	The HEP estimated (time: 1/3)
Rx trip	1.00E-3		
SIAS	1.87E-3		
CIAS	1.87E-3		
MSIS	1.87E-3		
CSAS	1.05E-3	4.75E-2	1.01E-1
RAS	1.87E-3	5.23E-2	1.15E-1
AFAS-1	3.68E-3	6.29E-2	1.47E-1
AFAS-2	3.68E-3	6.29E-2	1.47E-1
CDF	7.76E-6	8.00E-6	8.32E-6

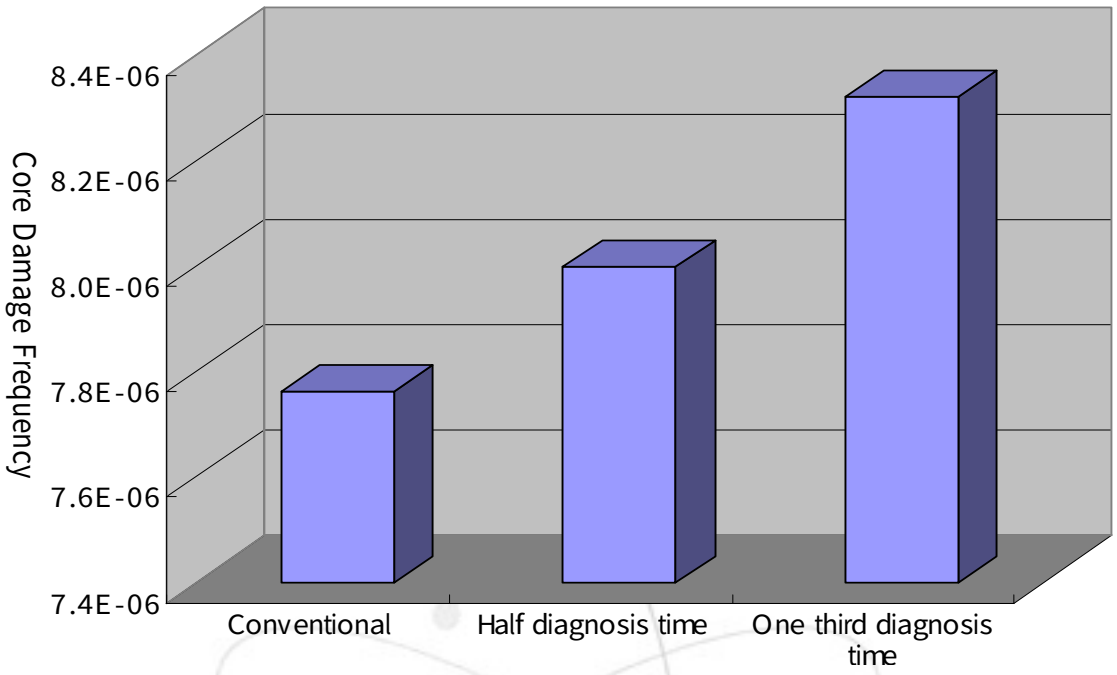

Figure 2. The information flow from the sensors to the reactor trip signal and the ESF signals through DPPS, DESFAS and operator in the KSNPP

2.4 Discussion

In this study, we investigated the failure probability of a manual actuation under the failure of instrumentation or automatic actuation systems. Since the HEP of a manual signal generation is a conditional probability given that the automatic signal generation fails, the operator would rely on the information provided by the sensors. In consideration of the various combinations of the sensor failures and the automatic signal generation system failures, we developed the simplified equations for estimating the effects of the conditions.

In the conventional analysis, the HEPs are estimated based on the assumption

of ‘normal condition of indications and alarms’. For the single-parameter safety signals, the analysis result reveals that the quantification of the HEP should be performed by focusing on the ‘no alarm from the automatic system and corresponding indications unavailable’ situation. Based on the KSNPP PSA model, we quantitatively performed the risk effect analysis of the HEPs for single-parameter signals regarding plant safety.

3. Condition-Based HRA (CBHRA)

A practical approach to develop a more realistic fault-tree model with a consideration of various conditions endured by a human operator is proposed in this chapter. As explained above chapters, in safety-critical systems, the generation failure of an actuation signal is caused by the concurrent failures of the automated systems and an operator action. These two sources of safety signals are complicatedly correlated. The failures of sensors or automated systems will cause a lack of necessary information for a human operator and result in error-forcing contexts such as the loss of corresponding alarms and indications. It is well known that the error-forcing contexts largely affect the operator's performance.

An automated system which consists of multiple processing channels and complex components is also affected by the availability of the sensors. This chapter proposes a condition-based human reliability assessment (CBHRA) method in order to address these complicated conditions in a practical way. We apply the CBHRA method to the manual actuation of the safety features such as a reactor trip and auxiliary feedwater actuation in Korean Standard Nuclear Power Plants. Even the human error probability of each given condition is simply assumed, the application results prove that the CBHRA effectively accommodates the complicated error-forcing contexts into the fault trees.

3.1 Concept of CBHRA

Quantification as part of a human reliability assessment involves the derivation of a probability distribution for basic events modeled in a PSA. In this study, each HEP consists of one unsafe action (*UA*) of which the probability is affected by the error forcing contexts (EFC). Given an accident scenario, the HEP (*H*) is calculated as [3], [9]:

$$H = \sum_i P(UA \mid EFC_i) P(EFC_i) \tag{6}$$

The same as in the analytic calculation in chapter 2, we consider two kinds of EFC: Alarms and sensor indications. For simplicity, the failure of display/actuation devices is not considered as an EFC. Since there are many redundant and diverse backups for these devices, we assume that the effect of their failure on the system's unavailability is relatively small.

Some alarms are generated by the automatic system of which a failure is also a reason for a signal generation failure. We have to consider both of signal generation failure reasons: Automated system failure and manual actuation failure. The failures of sensors are independent from the accident scenario. For sensors (*S*) and automatic systems (*A*), 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 (*F*) is calculated based on the HEP of Equation (6):

$$F = H = \sum_i \sum_j P(UA \mid A_i, S_j) P(A_i \mid S_j) P(S_j) \tag{7}$$

As shown in Equation (7), the human operator performance is affected by the automated signal generation system, and the failure of a system itself is one of the signal failure reasons. The relationship among the human operators, automatic systems, and instrumentation sensors is illustrated in Figure 3.

In the practical cases, the automatic systems consist of many components and input sensors. There are several redundant channels, and each channel processes the input signals from the corresponding sensors. Furthermore there are complicated voting processes and monitoring mechanisms in order to avoid the loss of the safety function in the case of a single component failure. The status of the instrumentation sensors affects the performance of both the automatic systems and the human operator in a complicated manner. If we have to construct a PSA model for all the combinations of these EFCs case by case, it would require a huge amount of effort, and its size would also be impractically large.

A fault tree is one of the favored methods by the PSA personnel. Based on the fault tree method, in order to take into acount the HEP issue with conditional events in a more effective manner, we propose the following steps of the CBHRA:

(1) Conducting an investigation into possible EFCs

(2) Selecting important EFCs

(3) Developing a set of conditions in consideration of selected EFCs

(4) Estimating the HEP for each condition

(5) Constructing a fault tree which includes one human error (HE) event for each manual action

(6) Obtaining minimal cut sets (MCS) by solving the fault tree

(7) Post-processing of MCSs

The purpose of steps (1) to (3) 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 (*n* groups) in order to treat them in a practical manner. Steps (5) and (6) are the same steps as in a conventional PSA approach. From the viewpoint of the HE event, after step (6), we can categorize the MCSs into several sets. The number of MCS sets equals to that of the HE events used in step (5).

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*'.

The manual implementation of step (7) is expected to require much effort. Therefore an automatic conditioning with a PSA software package is recommendable. An automatic conditioning could be enabled based on logical rules such as '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.

On the other hand, for the EOC, in order to distinguish the groups, the investigation into the event of AUTO_SUCESS is necessary. Generally, when we use a negation gate in the fault tree model, it is very hard to obtain the corresponding MCSs because the usual software packages require many resources and a long processing time to solve the negation logics. Therefore, for a practical use, the model of a single EOC event is preferable to that of the multiple EOC events. In addition to that, the probability of AUTO_SUCESS event could be assumed to be unity when the automated signal processing channels are highly reliable.

In the following sections, we will explain the application of the CBHRA method to the fault tree development for the generation failure of the safety signals in the KSNPP in a more detailed manner.

3.3 DPPS and DESFAS

In this study, two kinds of target safety signals are considered: Reactor trip signal and engineered-safety-feature (ESF) actuation signals which are the most important signals considered in the safety assessment of the KSNPP. Figure 3 shows the conceptual drawing of the information flow from the sensors to the target signals. In the KSNPP, there are seven ESFs and one reactor trip. Given a specific initiating event, each target signal could be generated by single or multiple trip parameters, and each parameter is instrumented by four redundant sensors.

Among the target safety signals, the reactor trip signal (RxTrip), safety injection actuation signal (SIAS), containment isolation actuation signal (CIAS) and main steam isolation signal (MSIS) are generated based on the instrumented value of the multiple parameters. On the other hand, the other signals, containment spray actuation signal (CSAS), recirculation actuation signal (RAS) and auxiliary feedwater actuation Signal–1 & 2 (AFAS-1 and AFAS-2) are generated based on the instrumented value of a single parameter.

As mentioned in the above sections, the signal processing channels and instrumentation channels are connected in a very complicated manner. Figure 4 shows the structure inside one of four processing channels of the DPPS. In the practical cases, therefore, the effective categorization of EFCs into several groups is the key to a successful modeling. If we consider every status of the signal processing system or instrumentation channels, there will be too many conditions to be modeled in the fault tree.

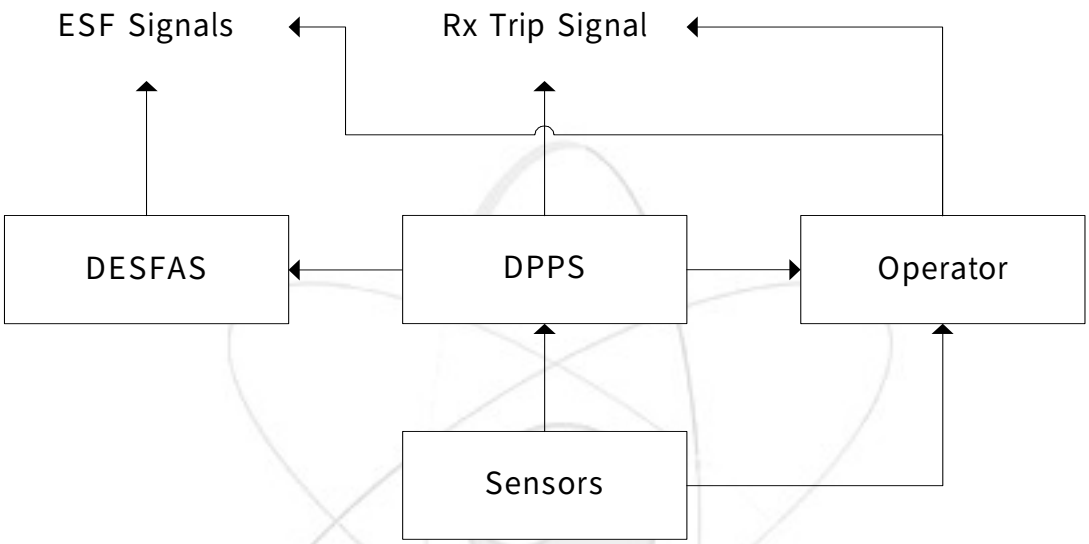

Figure 3. The information flow from the sensors to the reactor trip signal and the ESF signals through the DPPS, the DESFAS and an operator in the KSNPP

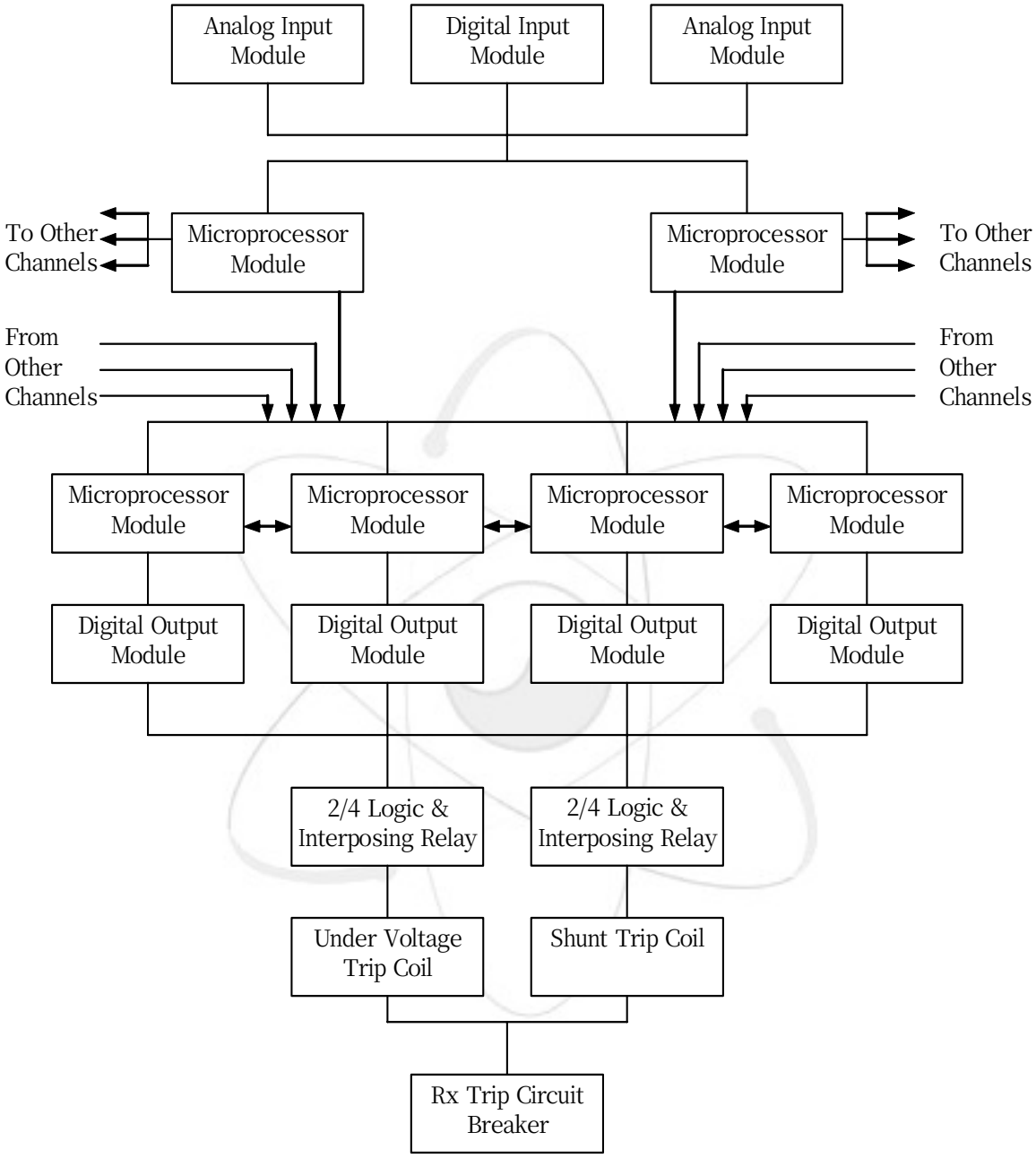

Figure 4. The structure inside a channel of the DPPS

There are two states regarding information delivered to the operator: Available or unavailable. Ambiguous states are not considered for simplicity. In the case of the KSNPP safety parameter, four independent instrumentation channels are displayed to the operator directly through the indication system and they are processed to generate the automatic safety-actuation signals and the alarms.

Regarding the availability of the alarms, the cases of two or more alarms out of four channels are considered as ‘alarm available’ status since the main function of an alarm is to make the operator recognize the abnormal situation. We assume that the operator might disregard the alarm from only one channel since he might consider it as a faulty alarm. Regarding instrumentation sensors, the cases of three or more normal (correct) channels are considered as ‘indication available’ status since the indications from two or less correct sensors are not enough to make a clear decision.

3.4 Application of CBHRA to the Single-Parameter Safety Function

In consideration of the two-out-of-four voting logic of the KSNPP, we can tabulate the availabilities of an automated safety signal, indication of the parameter and the alarms based on the status of the automated system and the instrumentation sensors. In the case of a single-parameter safety function, the results are shown in Table 3. The gray-colored cells are the EOC area in which the safety signals are automatically generated and the operator is expected not to interrupt them. The other cells indicate the EOO area in which the operator is expected to play actively the role of a backup for the automated system. For the single-parameter functions, we have two EOO conditions and one EOC condition.

There are two conditions in the EOC area. The probability of the condition 1* is very small when compared with that of condition 1. Even in the case that the automatic system is in an abnormal status, it is possible that there are two or more available processing channels. They should also be treated as EOC conditions. However, their probabilities are negligible comparing to that of condition 1. As explained in the above section, the single EOC event is suitable for a practical use. Therefore, it is reasonable to consider the condition 1 as the representative EOC condition.

Table 3. The conditions of a human error in the case of the 4-channel-single-parameter functions (O: available, X: unavailable)

Status of the automated system / Status of instrumentation	Normal	Abnormal
3 or more channels available	Auto. signal: O Indication: O Alarm: O *<Condition 1>*	Auto. signal: X Indication: O Alarm: X *<Condition 2>*
2 channels available	Auto. signal: O Indication: X Alarm: O *< Condition 1*>*	Auto. signal: X Indication: X Alarm: X *<Condition 3>*
1 or less channel available	Auto. signal: X Indication: X Alarm: X *<Condition 3>*	Auto. signal: X Indication: X Alarm: X *<Condition 3>*

The delicate quantification of the HEP in each condition especially the EOC probability is beyond the scope of this study. We apply rough assumptions based on discussions with HEP quantification experts in order to show the effect of the proposed

CBHRA method. Given a specific accident, the operator is assumed to spend a certain portion of the available diagnosis time to overcome the lack of information. That is, the operator is assumed to consume the given time for gathering the information from the other information sources.

In the case of condition 2, we assume that 30% of the diagnosis time will remain when the operator recognizes the situation under the trip/actuation alarms unavailable condition. In the case of condition 3, we assume that just 10% will remain.

The HEPs in this example application are not estimated based on database or software. In the conventional single HEP model, the information equipment is assumed to deliver the information to the operator. In this case, the operator could use 100% of the given time to diagnose the plant status. This HEP-100 is estimated for KSNPP using the THERP method [10] in consideration of several factors such as stress level, allowed time, sequence familiarity, etc. Based on this HEP-100, we recalculated the HEPs of 30% and 10% of diagnosis time (HEP-30 and HEP-10) with rough assumption that the HEP is governed by the diagnosis error. The shorten diagnosis time causes the increase of the HEP. We use Swain's nominal diagnosis model [8] for estimating the HEP-30 and the HEP-10.

The equipment failures are explicitly modeled in the fault tree. Therefore, the cutsets of signal generation failure consists of several equipment-failure events and a HE event. As explained in the previous section, this HE event is substituted by the properly conditioned HE event (HEP-30 or HEP-10) in consideration of equipment failure events in the cutset. For example, if there is the DPPS failure event and no

sensor failure event in the cutset, it corresponds to the condition 2 in Table 3. Then the HE event in that cutset should be substituted by HEP-30 event.

As shown in Figure 1, the signal failure probability could be obtained by the two events: The signal generation failure and the EOC. The EOC probability, the HEP in condition 1 is not considered in this study. For a demonstration purpose for the effect of the CBHRA method, we don't have to consider the EOC. In this study, therefore, we develop a model only for the signal generation failure.

As a typical single-parameter safety function, the AFAS is selected. When the steam generator water level goes under the setpoint, the DPPS/DESFAS automatically generates the AFAS in order to supply cooling water. Of course, the operator could also manually actuate the AFAS. Since the KSNPP includes two steam generators, there are two AFASs (AFAS-1 and AFAS-2).

Based on the fault tree models developed in previous studies [11],[12], we developed an AFAS-1 model which consists of 146 basic events and 206 logical gates. For the hardware equipment failure probabilities, we use the experienced data and the data provided by the vendors. Using KIRAP [13] which is a fault-tree analysis software package produced by the Korea Atomic Energy Research Institute, we analyze the developed plant-risk models.

Table 4 compares the dominant cutsets of the conventional single HEP method and the CBHRA. Since the HEP in condition 3 is much higher than that in condition 2, the common cause failure (CCF) of the sensors becomes the most dominant cutset in the CBHRA model. Figure 4 compares the calculated AFAS generation failure probabilities using the CBHRA method and the single HEP method. For the easy comparison, Figure 4 also shows the results from the cases of single HEP-30 and single HEP-10.

The result of CBHRA is calculated based on the HEPs for the conditions 1 to 3 in Table 3. The other results in Figure 5 are calculated using conventional single-human-error-event method. The CBHRA result, 1.25E-3, is significantly higher than the conventional result, 2.57E-5. This difference is caused by a consideration of the information availability. The CBHRA considers the lack of information as an EFC while a conventional analysis assumes that all the information could be delivered to the operator. The result also demonstrates the merit of the CBHRA method, a more sophisticated treatment of the EFCs.

Table 4. Dominant cutsets of the models developed using the CBHRA method and the single HEP method in the case of a single-parameter safety function (HE: Human error)

Modeling Method	Human Error	Component Failures	
CBHRA	HE-3	CCF of Sensors	
	HE-2	DESFAS Output Module Failure	
	HE-2	DESFAS Processor Module Failure	Watchdog Timer's Detection Failure
	HE-2	DESFAS Input Module Failure	
Single HEP	HE	DESFAS Output Module Failure	
	HE	CCF of Sensors	
	HE	DESFAS Processor Module Failure	Watchdog Timer's Detection Failure
	HE	DESFAS Input Module Failure	

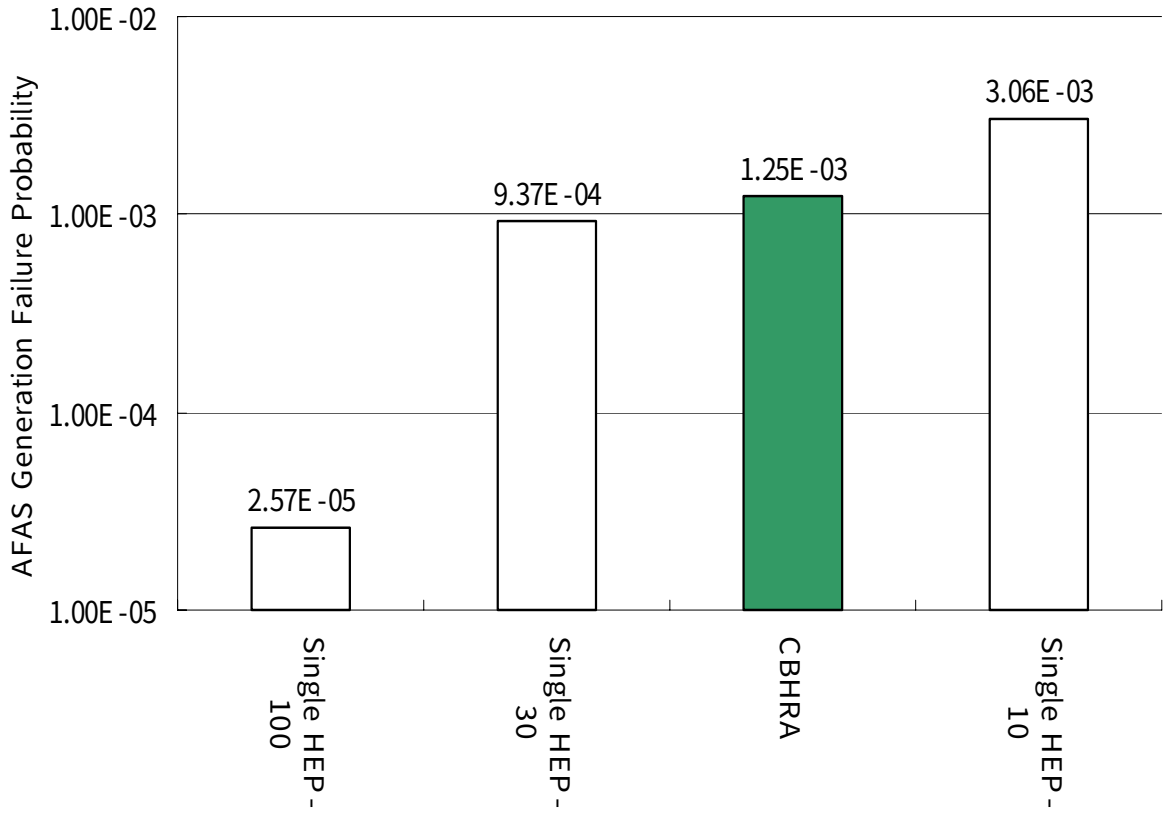

Figure 5. The comparison among the single HEP methods and the CBHRA method for the AFAS generation failure probabilities. Single HEP-100, 30 and 10 means that the single HEP method is used and the HEP is calculated based on the assumption that 100%, 30% and 10% of the diagnosis time is available, respectively. For the CBHRA, 30% and 10% is assumed to be available for the condition 2 and 3, respectively.

3.5 Application of CBHRA to the Multiple-Parameter Safety Function

In the case that the automated system operates normally, most conditions are EOC conditions. The only EOO condition is that all the parameters are unavailable in 3 or more channels. If there are one or more parameters of which 2 or more channels are available, the automated system will successfully generate a safety signal. That is, with a normal automated system, all the conditions of the instrumentation channels are considered as the EOC condition except for the only EOO condition of 'no available parameter which contains 2 or more normal channels'. For the EOC event, we use the condition that all the parameter indications are available since it is dominating.

On the other hand, in the case that the automated system is in an abnormal status, the automated safety signal and alarms are unavailable to the operator. Therefore, the only concern is the availability of the indications. Basically, there could be 2^n conditions (n: the number of parameters). If all the parameters are assumed to have a similar importance to the operator, the conditions will be expressed as; 'no indication available', '1-parameter indication available', '2-paramer indications available', …, 'n-parameter indications available'. In order to provide indications, 3 or more channels should be available for each parameter. The grouping illustrated in Table 5 is for the case of an equivalent importance. There are n+1 EOO conditions.

If some parameters are more important for the operator's decision making, their indication availabilities should be separately considered. In this case, we will have

more than n+1 but less than 2^n +1 EOO conditions according to the condition grouping strategy.

As a typical multiple-parameter safety function, the reactor trip signal is investigated in this study. Dissimilarly to the other safety functions, effective sensors for the reactor trip should be determined based on a careful consideration of the accident situation. In this study, we develop a model for the reactor trip signal generation failure under the small-loss-of-coolant-accident (SLOCA) condition. Based on an authors' previous study [6], we consider three parameters: Low departure from nucleate boiling ratio, low steam generator pressure, and high containment pressure.

Table 5. The conditions of a human error in the case of the 4-channel-multiple-parameter functions with the assumption of equivalently important parameters

(O: available, X: unavailable, NC: not concerned)

Status of the automated system / Status of instrumentation	Normal	Abnormal
All (*n*) parameters available (3 or more channels available for each available parameter)	Auto. signal: O Indication: O Alarm: O <*Condition 1*>	Auto. signal: X Indication: O Alarm: X <*Condition 2*>
n-1 parameters available (3 or more channels available for each available parameter)	Auto. signal: O Indication: NC Alarm: NC → <*Condition 1*>	Auto. signal: X Indication: (n-1)O, 1X Alarm: X <*Condition 3*>
…	Auto. signal: O Indication: NC Alarm: NC → <*Condition 1*>	Auto. signal: X Indication: … Alarm: X <*Condition …*>
1 parameter available (3 or more channels available)	Auto. signal: O Indication: NC Alarm: NC → <*Condition 1*>	Auto. signal: X Indication: 1O, (n-1)X Alarm: X <*Condition n*>
No parameter available (2 channels available for some parameters)	Auto. signal: O Indication: X Alarm: X → <*Condition 1*>	Auto. signal: X Indication: X Alarm: X <*Condition n+2*>
No parameter available (1 or less channel available for all parameters)	Auto. signal: X Indication: X Alarm: X <*Condition n+2*>	Auto. signal: X Indication: X Alarm: X <*Condition n+2*>

Based on the previous study [12], we developed a fault tree which consists of 182 basic events and 415 logical gates. The same assumptions and data as used for the AFAS-1 model are applied to this model. In addition to this, we assume the same importance among previous parameters. We assume that 30%, 23.3%, 16.7%, and 10% of diagnosis time will remain for conditions 2, 3, 4, and 5, respectively.

Figure 6 compares the reactor trip signal generation failure probabilities. The CBHRA result, 2.23E-6, is significantly higher than the conventional result, 2.51E-8. However, it almost equals to the result of the single HEP-30 model, 2.22E-6. This similarity implies that condition 2 overwhelms the other conditions in the case of a multiple-parameter safety function. That is, in this case, the single HEP with a consideration of the dominant condition would be an effective method.

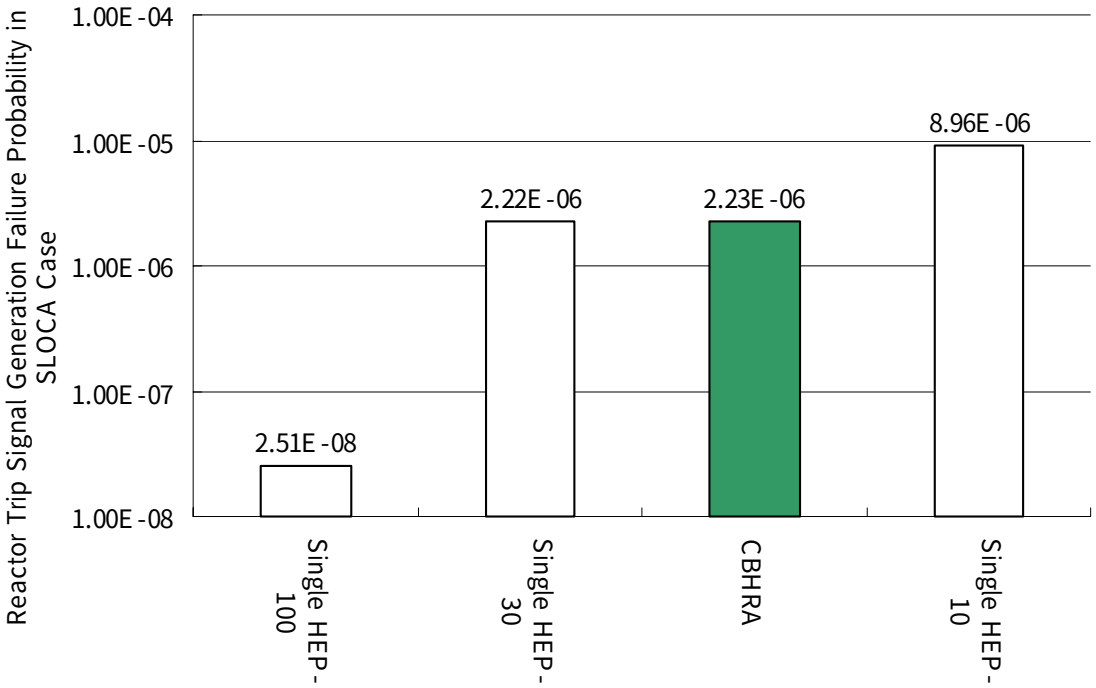

Figure 6. The comparison among the single HEP methods and the CBHRA method for the reactor trip signal generation failure probabilities.

3.6 Discussion

The failures of sensors or automated systems will cause a lack of necessary information for the operator's decision making. These are EFCs which should be considered in quantifying the HEP. In this study, the CBHRA method is proposed and we expect that it will provide an effective means for addressing the risk of complicate signal generation mechanisms which include a complex relationship among the automated system, the instrumentation sensors/indications and the human operator's manual actuation. The CBHRA method is applied to the manual actuation of the safety features such as a reactor trip and an auxiliary feedwater actuation in Korean Standard Nuclear Power Plants. The application results show that the CBHRA effectively accommodates the conditions.

In the case of conventional single HEP method, it is very hard to consider the multiple HE conditions. The merit of CBHRA is clearly shown in the application to the AFAS generation where no dominating HE condition exits. In this case, even if the HE conditions are carefully investigated, the single HEP method cannot accommodate the multiple conditions in a fault tree. On the other hand, the application result of the reactor trip in SLOCA shows that if there is a dominating condition, the use of single HEP method could be a practical way of developing a model.

In this study, we considered two EFCs: The parameter indications and the alarms. In order to be a more sophisticated and accurate method, however, the CBHRA should be able to accommodate various EFCs in addition to these. A practical method

for the quantification of HEPs in consideration of various EFCs should be developed. Further studies regarding these issues are recommendable.

4. Conclusion

Since the operator would rely on the information provided by the sensors and the alarms, the HEP of a manual signal generation is a conditional probability given that the automatic signal generation fails. The failures of sensors or automated systems will cause a lack of necessary information for the operator's decision making. The failures of sensors or automated systems will cause a lack of necessary information for a human operator and result in error-forcing contexts such as the loss of corresponding alarms and indications.

It is well known that the EFCs largely affect the operator's performance. These EFCs should be considered in quantifying the HEP. An automated system which consists of multiple processing channels and complex components is also affected by the availability of the sensors. In consideration of the various combinations of the sensor failures and the automatic signal generation system failures including the loss of alarms, we developed the practical method for accommodating the effects of the conditions.

In the conventional analysis, the HEPs are estimated based on the assumption of 'normal condition of indications and alarms'. In order to construct a more realistic signal-generation failure model, we have to consider more complicated conditions in a more realistic manner. In this study, we performed two kinds of investigation for addressing this issue.

One is the analytic calculations for estimating the effect of sensors failures on the system unavailability and plant risk. For the single-parameter safety signals, the analysis result reveals that the quantification of the HEP should be performed by focusing on the ‘no alarm from the automatic system and corresponding indications unavailable’ situation. Based on the KSNPP PSA model, we quantitatively performed the risk effect analysis of the HEPs for single-parameter signals regarding plant safety.

The other is the CBHRA method which is proposed for providing an effective means for addressing the risk of complicate signal generation mechanisms which include a complex relationship among the automated system, the instrumentation sensors/indications and the human operator’s manual actuation. The CBHRA method is applied to the manual actuation of the safety features such as a reactor trip and an auxiliary feedwater actuation in Korean Standard Nuclear Power Plants. The application results show that the CBHRA effectively accommodates the conditions.

In the case of conventional single HEP method, it is very hard to consider the multiple HE conditions. The merit of CBHRA is clearly shown in the application to the AFAS generation where no dominating HE condition exits. In this case, even if the HE conditions are carefully investigated, the single HEP method cannot accommodate the multiple conditions in a fault tree. On the other hand, the application result of the reactor trip in SLOCA shows that if there is a dominating condition, the use of single HEP method could be a practical way of developing a model.

In this study, we considered two EFCs: The parameter indications and the alarms. In order to be a more sophisticated and accurate method, however, the CBHRA should be able to accommodate various EFCs in addition to these. A practical method for the quantification of HEPs in consideration of various EFCs should be developed. Further studies regarding these issues are recommendable.

It is also notable that the effectiveness of the CBHRA method is quite correlated to the common-cause-failure modeling method. That is, if the common cause failures are treated in a more cautious manner, we could construct more realistic PSA model when we use the CBHRA method.

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] Hirschberg, S., Human Reliability Analysis in Probabilistic Safety Assessment for Nuclear Power Plants, CSNI Technical Opinion Papers, ISBN 92-64-02157-4, 2004.

[3] Forester, J., Bley, D., Cooper, S., Lois, E., Siu, N., Kolaczkowski, A., and Wreathall, J, Expert elicitation approach for performing ATHEANA quantification, Reliability Engineering and System Safety, Vol. 83, 2004.

[4] Kang, H.G. and Sung, T., An analysis of safety-critical digital systems for risk-informed design, Reliability Engineering and Systems Safety, Vol. 78, 2002.

[5] Min, K.R., et al., Reliability Study: KSNPP Reactor Protection System, KAERI/TR - 2164/02, Korea Atomic Energy Research Institute, 2002.

[6] Kang, H.G. and Jang, S.C. and Lim, H.G.., ATWS Frequency Quantification Focusing on Digital I&C Failures, Journal of Korea Nuclear Society, Vol. 36, 2004.

[7] Jang, S.C., Min, K.R., Han, S.H., Performance and Unavailability Analysis of RPS/ESFAS in Korea Standard Nuclear Power Plant, ICONE-10 Proceedings, Washington DC, USA, April 2002.

[8] Swain, A.D., Guttmann, H.E, Handbook of Human Reliability Analysis with

Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, 1983.

[9] US Nuclear Regulatory Commission (USNRC), Technical basis and implementation guidelines for a technique for human event analysis (ATHEANA), Washington, D.C., NUREG-1624 Rev. 1, 2000.

[10] Korea Hydro and Nuclear Power Company, Ulchin Units 3&4 Final Probabilistic Safety Assessment, 1995.

[11] Sudarno, W., et al., Reliability Study: Digital Engineered Safety Feature Actuation System of Korean Standard Nuclear Power Plant, KAERI/TR-2467/2003, Korea Atomic Energy Research Institute, 2003.

[12] Kang, H.G., et al., Reliability Study: Digital Reactor Protection System of Korean Standard Nuclear Power Plant, KAERI/TR-2419/2003, Korea Atomic Energy Research Institute, 2003.

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

APENDIX I.

Dominating cutsets of the AFAS signal generation failure by the operator and the automated system (DPPS) in the KSNPP

Reporting for GFSVAMA-AFAS1

value = 1.252e-003

Final Cut Sets

no	value	f-v	acc	cut sets		
1	4.516e-004		0.3607	0.3607	MFLTK-LSL1	FSOPH-C4	
2	2.989e-004		0.2387	0.5994	FSOMAV1A19	FSOPH-C3	
3	2.989e-004		0.2387	0.8381	FSOMAV2A19	FSOPH-C3	
4	6.655e-005		0.0531	0.8912	FSWDJV1A	FSPMAV1A	FSOPH-C3
5	6.655e-005		0.0531	0.9444	FSWDJV2A	FSPMAV2A	FSOPH-C3
6	1.867e-005		0.0149	0.9593	FSOMWDO	FSOPH-C3	
7	8.291e-006		0.0066	0.9659	FSPMW	FSWDJPCCF	FSOPH-C3
8	7.689e-006		0.0061	0.9721	FSIMWD	FSOPH-C3	
9	7.144e-006		0.0057	0.9778	FSORW	FSOPH-C3	
10	7.144e-006		0.0057	0.9835	RPOTW	FSOPH-C3	
11	3.741e-006		0.0030	0.9865	RPIMW	FSOPH-C3	
12	2.544e-006		0.0020	0.9885	FSPSRIRA	FSOMAV2A19	
13	2.544e-006		0.0020	0.9905	FSPSRIRA	FSOMAV1A19	
14	1.500e-006		0.0012	0.9917	RPPMWLL	RPWDJCCF	FSOPH-C3
15	1.331e-006		0.0011	0.9928	RPOMW	FSOPH-C3	
16	5.664e-007		0.0005	0.9932	FSPSRIRA	FSWDJV2A	FSPMAV2A
17	5.664e-007		0.0005	0.9937	FSPSRIRA	FSWDJV1A	FSPMAV1A
18	4.873e-007		0.0004	0.9941	RPOTAAB-AFAS1	FSORAAD-AFAS1	FSOPH-C3
19	4.873e-007		0.0004	0.9945	RPOTAAA-AFAS1	FSORAAC-AFAS1	FSOPH-C3
20	4.873e-007		0.0004	0.9949	RPOTAAA-AFAS1	RPOTAAC-AFAS1	FSOPH-C3
21	4.873e-007		0.0004	0.9953	FSORAAB-AFAS1	FSORAAD-AFAS1	FSOPH-C3
22	4.873e-007		0.0004	0.9956	RPOTAAB-AFAS1	RPOTAAD-AFAS1	FSOPH-C3
23	4.873e-007		0.0004	0.9960	FSORAAB-AFAS1	RPOTAAD-AFAS1	FSOPH-C3
24	4.873e-007		0.0004	0.9964	FSORAAA-AFAS1	FSORAAC-AFAS1	FSOPH-C3
25	4.873e-007		0.0004	0.9968	FSORAAA-AFAS1	RPOTAAC-AFAS1	FSOPH-C3
26	3.553e-007		0.0003	0.9971	MFLTYA-LSL1	MFLTYB-LSL1	MFLTYC-LSL1
	FSOPH-C4						
27	3.553e-007		0.0003	0.9974	MFLTYA-LSL1	MFLTYC-LSL1	MFLTYD-LSL1
	FSOPH-C4						

28	3.553e-007	0.0003	0.9977	MFLTYA-LSL1	MFLTYB-LSL1	MFLTYD-LSL1
	FSOPH-C4					
29	3.553e-007	0.0003	0.9979	MFLTYB-LSL1	MFLTYC-LSL1	MFLTYD-LSL1
	FSOPH-C4					
30	2.544e-007	0.0002	0.9981	FSPSW	FSOMAV2A19	
31	2.544e-007	0.0002	0.9983	FSPSW	FSOMAV1A19	
32	1.589e-007	0.0001	0.9985	FSPSRIRA	FSOMWDO	
33	9.898e-008	0.0001	0.9986	RPOTAAB-AFAS1	FSIMAV2A2	FSOPH-C3
34	9.898e-008	0.0001	0.9986	FSORAAD-AFAS1	FSIMAV2A1	FSOPH-C3
35	9.898e-008	0.0001	0.9987	RPOTAAC-AFAS1	FSIMAV1A1	FSOPH-C3
36	9.898e-008	0.0001	0.9988	FSORAAB-AFAS1	FSIMAV2A2	FSOPH-C3
37	9.898e-008	0.0001	0.9989	FSORAAC-AFAS1	FSIMAV1A1	FSOPH-C3
38	9.898e-008	0.0001	0.9989	RPOTAAD-AFAS1	FSIMAV2A1	FSOPH-C3
39	9.898e-008	0.0001	0.9990	RPOTAAA-AFAS1	FSIMAV1A2	FSOPH-C3
40	9.898e-008	0.0001	0.9991	FSORAAA-AFAS1	FSIMAV1A2	FSOPH-C3
41	7.056e-008	0.0001	0.9992	FSPSRIRA	FSPMW	FSWDJPCCF
42	6.544e-008	0.0001	0.9992	FSPSRIRA	FSIMWD	
43	6.080e-008	0.0000	0.9993	FSORW	FSPSRIRA	
44	6.080e-008	0.0000	0.9993	RPOTW	FSPSRIRA	
45	5.664e-008	0.0000	0.9994	FSPSW	FSWDJV1A	FSPMAV1A
46	5.664e-008	0.0000	0.9994	FSPSW	FSWDJV2A	FSPMAV2A
47	5.001e-008	0.0000	0.9994	RPPMWBI	FSOPH-C3	
48	3.118e-008	0.0000	0.9995	RPIMRA1	MFLTYB-LSL1	MFLTYD-LSL1
	FSOPH-C4					
49	3.118e-008	0.0000	0.9995	MFLTYA-LSL1	MFLTYB-LSL1	RPIMRD1
	FSOPH-C4					
50	3.118e-008	0.0000	0.9995	MFLTYA-LSL1	RPIMRB1	MFLTYC-LSL1
	FSOPH-C4					

APENDIX II.

Dominating cutsets of the reactor trip signal generation failure in SLOCA accident by the operator and the automated system (DPPS) in the KSNPP

Reporting for G-U5-SIG-SLOCA

value = 2.232e-006

Final Cut Sets

no	value	f-v	acc	cut sets
1	1.125e-006		0.5042	0.5042 RPPMWLL RPWDJCCF RPOPH-C2
2	9.983e-007		0.4473	0.9515 RPOMW RPOPH-C2
3	3.751e-008		0.0168	0.9683 RPPMWBI RPOPH-C2
4	1.302e-008		0.0058	0.9742 NRNEK RPIMW RPOPH-C2
5	9.798e-009		0.0044	0.9785 RPCCKCPC RPIMW RPOPH-C3
6	6.946e-009		0.0031	0.9817 RPUVW RPSHW
7	5.303e-009		0.0024	0.9840 RCVTK RPIMW RPOPH-C2
8	3.872e-009		0.0017	0.9858 RCTTKRCLO RPIMW RPOPH-C2
9	3.872e-009		0.0017	0.9875 RCTTKRCHI RPIMW RPOPH-C2
10	1.826e-009		0.0008	0.9883 NRNEK CMPTK-HCP RCPTK-LPP RPOPH-C4
11	1.246e-009		0.0006	0.9889 RPCCKCPC CMPTK-HCP RCPTK-LPP RPOPH-C5
12	1.113e-009		0.0005	0.9894 RPUVW RPSHDA RPSHDC
13	1.113e-009		0.0005	0.9899 RPUVW RPSHDB RPSHDD
14	9.428e-010		0.0004	0.9903 RPRTK RPIMW RPOPH-C2
15	7.439e-010		0.0003	0.9906 RCVTK CMPTK-HCP RCPTK-LPP RPOPH-C4
16	5.432e-010		0.0002	0.9909 RCTTKRCHI CMPTK-HCP RCPTK-LPP RPOPH-C4
17	5.432e-010		0.0002	0.9911 RCTTKRCLO CMPTK-HCP RCPTK-LPP RPOPH-C4
18	4.083e-010		0.0002	0.9913 NRNEYA NRNEYB NRNEYD RPIMW RPOPH-C2
19	4.083e-010		0.0002	0.9915 NRNEYA NRNEYC NRNEYD RPIMW RPOPH-C2
20	4.083e-010		0.0002	0.9917 NRNEYA NRNEYB NRNEYC RPIMW RPOPH-C2
21	4.083e-010		0.0002	0.9918 NRNEYB NRNEYC NRNEYD RPIMW RPOPH-C2
22	2.335e-010		0.0001	0.9920 RPEDKSPC RPIMW RPOPH-C2
23	1.669e-010		0.0001	0.9920 NRNEYA NRNEYB RCVTYC RPIMW RPOPH-C2
24	1.669e-010		0.0001	0.9921 NRNEYB NRNEYC RCVTYD RPIMW RPOPH-C2

25	1.669e-010	0.0001	0.9922	NRNEYA	NRNEYB	RCVTYD	RPIMW	RPOPH-C2
26	1.669e-010	0.0001	0.9923	NRNEYA	NRNEYC	RCVTYD	RPIMW	RPOPH-C2
27	1.669e-010	0.0001	0.9923	RCVTYB	NRNEYC	NRNEYD	RPIMW	RPOPH-C2
28	1.669e-010	0.0001	0.9924	RCVTYA	NRNEYC	NRNEYD	RPIMW	RPOPH-C2
29	1.669e-010	0.0001	0.9925	RCVTYA	NRNEYB	NRNEYD	RPIMW	RPOPH-C2
30	1.669e-010	0.0001	0.9926	NRNEYA	RCVTYC	NRNEYD	RPIMW	RPOPH-C2
31	1.669e-010	0.0001	0.9926	RCVTYA	NRNEYB	NRNEYC	RPIMW	RPOPH-C2
32	1.669e-010	0.0001	0.9927	NRNEYA	RCVTYB	NRNEYC	RPIMW	RPOPH-C2
33	1.669e-010	0.0001	0.9928	NRNEYB	RCVTYC	NRNEYD	RPIMW	RPOPH-C2
34	1.669e-010	0.0001	0.9929	NRNEYA	RCVTYB	NRNEYD	RPIMW	RPOPH-C2
35	1.322e-010	0.0001	0.9929	RPRTK	CMPTK-HCP		RCPTK-LPP	
	RPOPH-C4							
36	1.219e-010	0.0001	0.9930	NRNEYA	RCTTYRCLOC		NRNEYD	RPIMW
	RPOPH-C2							
37	1.219e-010	0.0001	0.9930	NRNEYA	NRNEYB	RCTTYRCHIC		RPIMW
	RPOPH-C2							
38	1.219e-010	0.0001	0.9931	NRNEYA	RCTTYRCLOB		NRNEYD	RPIMW
	RPOPH-C2							
39	1.219e-010	0.0001	0.9931	NRNEYB	NRNEYC	RCTTYRCLOD		RPIMW
	RPOPH-C2							
40	1.219e-010	0.0001	0.9932	NRNEYA	RCTTYRCHIC		NRNEYD	RPIMW
	RPOPH-C2							
41	1.219e-010	0.0001	0.9932	NRNEYB	NRNEYC	RCTTYRCHID		RPIMW
	RPOPH-C2							
42	1.219e-010	0.0001	0.9933	NRNEYA	NRNEYC	RCTTYRCHID		RPIMW
	RPOPH-C2							
43	1.219e-010	0.0001	0.9933	RCTTYRCHIA		NRNEYB	NRNEYD	RPIMW
	RPOPH-C2							
44	1.219e-010	0.0001	0.9934	RCTTYRCHIB		NRNEYC	NRNEYD	RPIMW
	RPOPH-C2							
45	1.219e-010	0.0001	0.9935	RCTTYRCLOA		NRNEYC	NRNEYD	RPIMW
	RPOPH-C2							
46	1.219e-010	0.0001	0.9935	RCTTYRCLOA		NRNEYB	NRNEYC	RPIMW
	RPOPH-C2							
47	1.219e-010	0.0001	0.9936	RCTTYRCLOB		NRNEYC	NRNEYD	RPIMW
	RPOPH-C2							
48	1.219e-010	0.0001	0.9936	NRNEYA	NRNEYC	RCTTYRCLOD		RPIMW

	RPOPH-C2						
49	1.219e-010	0.0001	0.9937	NRNEYA	RCTTYRCHIB	NRNEYD	RPIMW
	RPOPH-C2						
50	1.219e-010	0.0001	0.9937	RCTTYRCHIA	NRNEYB	NRNEYC	RPIMW
	RPOPH-C2						

서 지 정 보 양 식					
수행기관보고서번호	위탁기관보고서번호		표준보고서번호		INIS 주제코드
KAERI/TR-2467/2003					
제목 / 부제	디지털 특성을 반영한 조건기반 인간신뢰도분석 방법론 연구				
연구책임자 및 부서명 (AR,TR 경우 주저자)	강현국 (종합안전평가부)				
연 구 자 및 부 서 명	엄흥섭, 장승철, 하재주 (종합안전평가부)				
출 판 지	대전	발행기관	한국원자력연구소	발행년	2005 년 5 월
페 이 지	65p.	도 표	있음(O), 없음( )	크 기	A4
참고사항					
비밀여부	공개(O), 대외비( ), __ 급비밀		보고서종류		기술보고서
연구위탁기관	과학기술부		계약 번호		
초록(15-20 줄 내외)					

인적 오류(Human Error)의 확률론적 추정은 원자력발전소 전체의 확률론적 안전성 평가(Probabilistic Safety Assessment; PSA)에 매우 큰 영향을 미친다. 한편 최근 국내 표준원전에 도입되고 있는 디지털 안전계통은 디지털 기술의 특성상 다중의 기능을 동시에 수행하게 되므로 디지털 안전계통의 고장이 인적오류에 영향을 미쳐 궁극적으로 플랜트 전체의 안전성에 영향을 미칠 수 있으므로 이에 대한 상세 분석이 필요하다. 기존의 고장수목을 이용한 PSA 모델에서는 사고상황에서도 운전원에게는 모든 정보가 정상적으로 전달되는 것을 가정하여 단일사건으로 인적오류를 취급하였으나, 보다 정확한 분석을 위해서는 이러한 상세분석을 바탕으로 현실적인 모델을 개발할 필요가 있다.

본 연구에서는 이러한 고장의 파급과 인적 오류 증가의 가능성을 정량적으로 평가하고 고장수목 모델에 반영하기 위한 방법론을 제시하였다. 먼저 해석적인 방법으로 기존의 단일조건 단일사건 모델의 타당성을 검토하였다. 검토결과 기존의 방법은 다중변수 안전기능에서는 비교적 근사적인 분석이 가능하나, 단일변수 안전기능의 경우에는 분석결과가 큰 차이를 보이는 것을 확인하였다.

따라서 본 연구에서는 '조건부 인적 오류 정량화(CBHRA)' 방법을 개발하였다. 인간 운전원이 당면하는 모든 상황에 대해 조건을 정하여 분석하는 것이 가장 정확한 분석방법이긴 하나 실제로 적용하기에는 큰 어려움이 있으므로, 이러한 상황을 디지털계통의 고장과 센서의 고장 등을 고려하여 몇개의 그룹으로 간략화하여 인적오류 확률을 산정한 후, 그 값을 기존의 단일 인적오류 사건 고장수목에 반영시키는 방법론을 제시하였다.

이렇게 개발된 CBHRA 방법론을 한국형 표준원전에 적용한 결과를 통해 이 방법의 유효성과 타당성을 검증하였다.

주제명 키워드 (10 단어내외)	조건분 인적오류 정량화(CBHRA), 확률론적 안전성 평가(PSA), 위험도 정보 활용(RIA), 디지털 안전계통

BIBLIOGRAPHIC INFORMATION SHEET					
Performing Org. Report No.	Sponsoring Org. Report No.	Standard Report No.	INIS Subject Code		
KAERI/TR-2907/2005					
Title / Subtitle	Condition-based Human Reliability Assessment for Digitalized Control Room				
Main Author	H.G. Kang (Integrated Safety Assessment Team)				
Researcher and Dept.	S.C. Jang, H.S. Eom, J.J. Ha (Integrated Safety Assessment Team)				
Publication Place	Daejeon	Publisher	KAERI	Publication Date	2005.5
Page	65p.	Fig. & Tab.	Yes(O), No( )	Size	A4
Note					
Classified	Open(O), Restricted( ), ___ Class Document			Report Type	Technical Report
Sponsoring Org.	MOST			Contract No	

Abstract (15-20 Lines)

In safety-critical systems, the generation failure of an actuation signal is caused by the concurrent failures of the automated systems and an operator action. These two sources of safety signals are complicatedly correlated. The failures of sensors or automated systems will cause a lack of necessary information for a human operator and result in error-forcing contexts such as the loss of corresponding alarms and indications. In the conventional analysis, the human error probabilities (HEP) are estimated based on the assumption of 'normal condition of indications and alarms'. In order to construct a more realistic signal-generation failure model, we have to consider more complicated conditions in a more realistic manner. In this study, we performed two kinds of investigation for addressing this issue.

We performed the analytic calculations for estimating the effect of sensors failures on the system unavailability and plant risk. For the single-parameter safety signals, the analysis result reveals that the quantification of the HEP should be performed by focusing on the 'no alarm from the automatic system and corresponding indications unavailable' situation.

This study also proposes a condition-based human reliability assessment (CBHRA) method in order to address these complicated conditions in a practical way. We apply the CBHRA method to the manual actuation of the safety features such as a reactor trip and auxiliary feedwater actuation in Korean Standard Nuclear Power Plants.

In the case of conventional single HEP method, it is very hard to consider the multiple HE conditions. The merit of CBHRA is clearly shown in the application to the AFAS generation where no dominating HE condition exits. In this case, even if the HE conditions are carefully investigated, the single HEP method cannot accommodate the multiple conditions in a fault tree. On the other hand, the application result of the reactor trip in SLOCA shows that if there is a dominating condition, the use of single HEP method could be a practical way of developing a model.

Subject Keywords (About 10 words)	Probabilistic Safety Assessment (PSA), Condition-based HRA (CBHRA) Risk-informed application (RIA), Safety-Critical Digital System