A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants

Man Cheol Kim*, Poong Hyun Seong

Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 373-1, Guseong-dong, Yuseong-gu, Daejeon 305-701, South Korea

Received 12 January 2005; accepted 16 April 2005
Available online 5 July 2005

Abstract

To make probabilistic safety assessment (PSA) more realistic, the improvements of human reliability analysis (HRA) are essential. But, current HRA methods have many limitations including the lack of considerations on the interdependency between instrumentation and control (I&C) systems and human operators, and lack of theoretical basis for situation assessment of human operators. To overcome these limitations, we propose a new method for the quantitative safety assessment of I&C systems and human operators. The proposed method is developed based on the computational models for the knowledge-driven monitoring and the situation assessment of human operators, with the consideration of the interdependency between I&C systems and human operators. The application of the proposed method to an example situation demonstrates that the quantitative description by the proposed method for a probable scenario well matches with the qualitative description of the scenario. It is also demonstrated that the proposed method can probabilistically consider all possible scenarios and the proposed method can be used to quantitatively evaluate the effects of various context factor on the safety of nuclear power plants. In our opinion, the proposed method can be used as the basis for the development of advanced HRA methods.

Keywords: Nuclear power plant; Probabilistic safety assessment; Human reliability analysis; I&C system; Bayesian network; Information theory; Context factors

1. Introduction

Needless to say, safety is one of the most important concerns in the design and operation of nuclear power plants (NPPs). Currently, quantitative safety analysis is mainly performed in the framework of probabilistic safety assessment (PSA). As the regulatory environment moves to the risk-informed regulation and application, PSA will become the basis for a lot of decision making for the operation of NPPs. It means that as the PSA becomes more realistic, we can achieve higher safety and economy.

PSA framework is so well established, and therefore there is little controversy on its methodology, except human reliability analysis (HRA). Actually, human operators take an important part in the safety of NPPs. In a study, it was found that human error probability has about 58% contribution to core damage frequency (CDF) [1]. Importance analysis in the probabilistic safety analysis (PSA) for Ulchin 3&4 nuclear power plants (located in Republic of Korea) reveals that human failure events take five positions among the top 10 most important basic events [2]. Beside these, a lot of literatures emphasize the importance of human failures or human errors in qualitative or quantitative ways. Due to the importance of HRA in the PSA framework, HRA is considered as the bottleneck to the improvement of PSA.

In the viewpoint of HRA, human performance is mainly affected by situation assessment, since most important and difficult thing is the situation assessment to select appropriate procedure or mitigating task [2]. In this sense, the situation assessment of human operators in accident situations should be considered to be most important in HRA, and therefore it should be analyzed on the firm basis of situation assessment models. But, in most conventional (first generation) HRA methods such as THERP [3], ASEP [4], HCR [5], and HEART [6], the methods for estimating
the failure probabilities of situation assessment are mainly based on estimations based on time–reliability curves determined by expert consensus, with modifications by the effects of performance shaping factors (PSFs) such as stress and training. It means that those methods do not pay enough attentions to the situations in which operators have to perform the situation assessment, and this becomes one source of a lot of criticisms on the conventional HRA methods. As a result, conventional HRA methods have limitations in considering the possibility of operators’ unsafe actions due to wrong situation assessment (so called errors-or-commission in many literatures).

Even though advanced (second generation) HRA methods such as CREAM [7] and ATHEANA [8] proposed various approaches to consider the situations or the contexts in which operators have to perform the situation assessment, we propose a new approach to consider the situations or contexts.

2. Interdependency of I&C systems and human operators

2.1. Conventional model for I&C systems and human operators

Fig. 1 shows a simplified fault tree to show how the current PSA technology models the failure of generating the safety injection actuation signal (SIAS) in accident situations. As can be seen in Fig. 1, the failure of generating SIAS is modeled to be caused by the failure of both automatic and manual generation of SIAS. It can be also seen that the automatic generation of SIAS and manual generation of SIAS are assumed to be independent. Even though some simple dependencies have been considered in current PSAs such as when a fault in the automatic circuit(s) may prevent the manual signal from being properly processed thereby failing the manual signal as well, typically the loss of the sensor/indication (both affecting automatic action and the manual response) is often not explicitly treated. Therefore, it can be said that the automatic control signals generated by I&C systems and manual control signals generated by human operators are often assumed to be independent in the current PSA technology.

As mentioned before, human performance in accident situations is mainly affected by situation assessment. In this sense, the estimation of the human failure probabilities for the situation assessment in accident situations is one of the most important parts in HRA. Fig. 2 shows how conventional HRA methods estimate the human failure probabilities for the situation assessment in accident situations. In case of ASEP or THERP, the nominal diagnosis error probabilities are estimated using the time–reliability curve shown in Fig. 2(a), and then modified by various performance shaping factors (PSFs). In case of HCR, the time–reliability curve shown in Fig. 2(b) is used. In general, the allowable time and/or the type of the tasks are considered to be dominant factors in estimating the human failure probabilities for the situation assessment in accident situations in conventional HRA methods.

2.2. Dependency of I&C systems on human operators

It is mentioned that the current PSA technology assumes that the automatic control signals generated by I&C systems and manual control signals generated by human operators are independent. In this sense, the generation of automatic SIAS in the fault tree shown in Fig. 1 will not be affected by human operators. This means that even though human

---

**Fig. 1. Simplified fault tree for the failure of generating the safety injection actuation signal (SIAS) in accident situations.**
operators fail to understand the accident situation correctly, it is assumed that the automatic generation of SIAS will not be affected by the misunderstanding of human operators.

But, we think that this assumption is somewhat too optimistic, because there are certainly a lot of possibilities for human operators to bypass the automatic generation of control signals such as SIAS, appropriately or inappropriately. A representative example of such possibilities is the reduction of high-pressure safety injection flow by human operators in Three Mile Island (TMI) accident. Analysis of recent incident reports also reveals that operators sometimes bypass safety functions when they cannot clearly understand the situation, with a hope that they can manage the situation. An AEOD report which identified 14 inappropriate bypasses of engineered safety features (ESFs) over 41 months supports this operators’ tendency [9]. In this sense, we believe that the reliabilities of automatic control signals for mitigating accident situations generated by I&C systems should be considered to be dependant on the situation assessment of human operators. Based on this belief, we also think that the importance of the situation assessment of human operators in accident situations should be emphasized more.

2.3. Dependency of human operators on I&C systems

Situation assessment can be explained as the process of accumulating the situation awareness (the degree of understanding the situation correctly) based on their knowledge, which is formed from training and experience, and the information that they receive. Considering the fact that the I&C systems are a major source of information to main control room (MCR) operators, we believe that the situation assessment of human operators should be considered to be dependent on I&C systems.

The concept of risk concentration on I&C systems by Kang and Jang [10] emphasizes the dependency of human operators on I&C systems. The major point of the concept is that the failure of one safety–critical digital system in an NPP not only leads to the failure of generating the reactor trip signal and necessary control signals for mitigating accident situations, but also possibly deteriorates the generation of manual control signals by human operators because the digital system possibly also fails to generate necessary alarms for human operators.

Even though we agree with the possibilities of that kind of situations, we are more concerned about the effects of instrument faults to the situation assessment of human operators. A sensitivity analysis of a quantitative model integrating the I&C system, man–machine interface (MMI), and human operators, developed by Kim and Seong [11], shows that the reliability of instruments and factors related to human operators are important to the generation of necessary control signals. The effects of instrument faults on the situation assessment of human operators are also emphasized repeatedly in ATHEANA [8].

2.4. Interdependency between I&C systems and human operators

Above two sections describe the dependency of the I&C systems on human operators and the dependency of human operators on I&C systems. Therefore, it can be said that I&C systems and human operators are interdependent. But, as mentioned above, the current PSA technology often assumes that I&C systems and human operators are independent. As a result, the quantitative models for the situation assessment of human operators shown in Fig. 2 cannot incorporate the interdependency of I&C systems and human operators.

To incorporate the interdependency of I&C systems and human operators, we believe that the current PSA technology should be modified and more advanced quantitative models for the situation assessment of human operators in accident situations, compared to those of conventional HRA methods, are necessary.
3. The proposed method

Fig. 3(a) shows how I&C systems and human operators are generally considered in the current PSA technology. As can be seen in Fig. 3(a), the manual control by human operators is modeled to be independent on sensors, which are a part of I&C systems. Even though it is not clearly shown in Fig. 3(a), the automatic control signals generated by control/protection systems, which are also a part of I&C systems, should be modeled to be independent on the manual control signals generated by human operators.

Fig. 3(b) shows how I&C systems and human operators are considered in the proposed method. In Fig. 3(b), the manual control is modeled to be dependent on the situation assessment of human operators, which is also modeled to be dependent on the information that operators receive from the sensors through indicators. In this way, the dependency of human operators on I&C systems can be modeled. By modeling the automatic control signals generated by control/protection systems can be overruled by the manual control signals by human operators, the dependency of I&C systems on human operators can be modeled.

3.1. Modeling of information processing by human operators

We know how information is processed in I&C systems, but we do not know how information is processed in human operators. Even though many situation awareness models such as Endsley [12], Bendy and Meister [13], and Adams et al [14] have been developed, and they can be used to explain how information is processed by human operators, there are a lot of limitations to use those models to describe how human operators process the information they receive, due to their qualitative and descriptive nature. Among several quantitative situation assessment models such as Miao et al. [15] and Kim and Seong [16], we believe that Kim and Seong [16] is appropriate to quantitatively describe how human operators process the information they receive.

3.2. Mathematical modeling of I&C systems and human operators

The mathematical model for the I&C systems and human operators when the interdependency between I&C systems and human operators are considered is similar to the mathematical model used in Kim and Seong [16]. Fig. 4 briefly summarizes the structure of the proposed model and the definitions of the variables. W indicates the plant state (the situation), Z\_i (i=1,2,...,m) indicate various sensors, and Y\_i indicate various indicators. X indicates operators’ situation model, V indicates the manual control signal, and U indicates the control signal. In mathematical forms, the variables are defined as follows:

\[ W = \{w_1, w_2, \ldots, w_l\} \] (1)

\[ Y_i = \{y_{i1}, y_{i2}, \ldots, y_{id}\} \quad \text{where } i = 1, 2, \ldots, m. \] (2)

\[ Z_i = \{z_{i1}, z_{i2}, \ldots, z_{id}\} \quad \text{where } i = 1, 2, \ldots, m. \] (3)

\[ X = \{x_1, x_2, \ldots, x_l\} \] (4)

\[ V = \{v_1, v_2, \ldots, v_j\} \] (5)

\[ U = \{u_1, u_2, \ldots, u_g\} \] (6)
Similarly to Kim and Seong [16], we assume the following two assumptions for operators’ mental model.

1. Different kinds of plant state can be modeled to be mutually exclusive.
2. Operators have deterministic rules on the dynamics of the plant.

The deterministic rules on the dynamics of the plant can be described using conditional probabilities, as follows:

$$P(y_{ij}|x_k) = \begin{cases} 1 & \text{if } y_{ij} \text{ is expected upon } x_k \\ 0 & \text{if } y_{ij} \text{ is not expected upon } x_k \end{cases} \quad (7)$$

The situation assessment of human operators is quantitative described using Bayesian inference. The details of the explanation are described in Kim and Seong [16].

$$P(x_k|y_{ij}) = \frac{P(y_{ij}|x_k)P(x_k)}{\sum_{i=1}^m P(y_{ij}|x_k)P(x_k)} \quad (8)$$

And the process or knowledge-driven monitoring is described based on the expected information from each indicator, which can be calculated based on the information theory. The details of the explanation are described in Kim and Seong [17]. The expected information from an indicator $$Y_i$$ is given as follows

$$T(X; Y_i) = H(X) + H(Y_i) - H(X, Y_i) \quad (9)$$

where

$$H(A) = \sum_i p(a_i) \log_2 \frac{1}{p(a_i)}.$$

The manual control is assumed to be determined by the situation model of human operators. It is assumed that the relations between the situation model of human operators and the manual control are also deterministic. For example, if human operators believe that a loss of coolant accident (LOCA) occurs in the plant but the reactor trip is not actuated, it is assumed that human operators always decide to actuate manual reactor trip.

But, the possibilities of action errors, e.g. push a wrong button, in the manual control should be considered, and they define conditional probabilities, $$P(v_i|x_k)$$ ($$i=1,2,...,f$$ and $$k=1,2,...,l$$) in the mathematical model for the manual control. The estimation of the action errors probabilities, which determine $$P(v_i|x_k)$$s, follows conventional HRA methods such as ASEP, THERP, HCR and so on.

The reliabilities of I&C systems, which consists of sensors and control/protection systems in Fig. 4, can be calculated using the fault tree analysis, but we think that the analysis can become easier when the reliability graph with general gates (RGGG) [18] is used. The reliabilities of I&C systems are used to determine conditional probabilities, $$P(u_k|v_i, z_{1j}, ..., z_{mj})$$ ($$k=1,2,...,g$$, $$i=1,2,...,f$$ and $$k=1,2,...,n$$).

Therefore, the probability distribution for the control signal $$U$$ can be determined based on the plant state $$W$$ and conditional probabilities.

4. An example

4.1. Example situation

To demonstrate the feasibility of the proposed method, we apply the proposed method to an example situation. The example situation is a LOCA with common cause failure of pressurizer pressure sensors in a pressurized water reactor (PWR) plant. We use the compact nuclear simulator (CNS) which was originally developed by Korea Atomic Energy Research Institute (KAERI) and Studsvik Inc., and recently renewed by KAERI [19]. The reference plants of CNS are Kori 3&4 nuclear power plants which are Westinghouse 900 MWe 3-loop pressurized water reactors (PWRs).

By modifying the simulation code, we fix the parameter for the pressurizer pressure measured by sensors to...
the normal operation value. The physical meaning of the modification is the occurrence of the common cause failure (CCF) of 4 pressurizer pressure sensors. In this situation, we induce a small loss of coolant accident (SLOCA) with a break size of 5 cm². Fig. 5 shows the trends of various plant parameters. The left-above trend graph in Fig. 5 shows the trends of the actual pressurizer pressure and that of the pressurizer pressure measured by failed sensors. It can be seen that the measured pressurizer pressure does not change, even though the actual pressurizer pressure decreases continuously. Because the measured pressurizer pressure does not change, the automatic reactor trip signal by low pressurizer pressure criterion will not be generated by reactor protection system (RPS).

In this situation, the generation of the automatic reactor trip signal by the over-temperature delta-\(T\) (OT\(\Delta\)T) criterion is expected. The right-above trend graph in Fig. 5 shows the calculated OT\(\Delta\)T and its trip setpoint, and indicates that the calculated OT\(\Delta\)T is always below the setpoint, which means that automatic reactor trip signal by the OT\(\Delta\)T criterion will not be generated. Because the measured pressurizer pressure is also used to calculate the OT\(\Delta\)T, the CCF of pressurizer pressure sensors also prohibits the RPS from generating the reactor trip signal by the OT\(\Delta\)T criterion. Due to the failure of generating reactor trip signal by the two criteria, the reactor trip will not occur and the accident continues to proceed. The left-below trend graph in Fig. 5 shows the decrease of the pressurizer level and the setpoint for low pressurizer level alarm generation. The right-below trend graph in Fig. 5 shows the average temperature of the reactor coolant system, \(T_{avg}\), and the reference temperature determined by turbine load, \(T_{ref}\).

Due to the failure of pressurizer pressure sensors, the safety injection (SI) signal by low pressurizer pressure will not be generated by the engineered safety features actuation system (ESFAS). It means that the common cause failure of pressurizer pressure sensors can simultaneously prohibit the RPS from generating the reactor trip signal and the ESFAS from generating the SI signal. In this situation, operators can see several alarms generated by control systems and alarm systems, which inform the operators the occurrence of an abnormal situation. Fig. 6 shows the generated alarms for the situation described above. The role of operators in this situation is to correctly recognize the occurrence of an accident and generate the manual reactor trip signal and SI actuation signals, and follow the emergency operation procedures (EOPs). Even though there are several symptoms that indicate the occurrence of a LOCA such as the decrease in the pressurizer level and the increase in the containment radiation, whether operators can correctly recognize the occurrence of an accident is quite unknown. In the viewpoint of PSA, what is important is the probability that human operators correctly recognize the occurrence of an accident and generate the manual reactor trip signal or the SI actuation signal. But, as mentioned above, conventional HRA methods cannot provide appropriate

![Fig. 5. Trends of various plant parameters by CNS for the example situation.](image-url)
probabilities for such situations described above, since they only take the allowable time or the type of tasks (skill-based, rule-based or knowledge-based) as dominant factors.

4.2. A probable scenario

Before the operators recognize the occurrence of the accident, operators might think that the plant is in the state of normal operation. As shown in Fig. 6, the human operators receive the containment radiation high alarm at 49 s after the occurrence of the accident, because the LOCA is inserted into the simulator at 0:3:00. Then, the human operators will move to the containment radiation indicator and observe that the containment radiation is increasing. This is an example of data-driven monitoring. In this situation they will think two possibilities, the failure of containment radiation sensors or indicators in normal operation or the occurrence of a LOCA. To understand the situation more clearly, they will decide to monitor other indicators. This is the process of knowledge-driven monitoring. If they observe that pressurizer pressure does not change, due to the CCF of pressurizer pressure sensors, they might understand the situation as the failure of containment radiation sensors or indicators in normal operation. But, to make sure their understanding of the situation more clearly, they might see other indicators. If they observe that the reactor power is decreasing, they might think of the possibility of the occurrence of a LOCA, and therefore actuate manual reactor trip and safety injection. Even though the human operators think of the possibility of a LOCA, it is expected that they cannot make sure the occurrence of a LOCA at this point. Therefore, it is also expected that the human operators monitor more indicators to understand the situation more clearly.

4.3. Quantitative analysis for the scenario

Fig. 7 is a quantitative model for the example situation. For simplicity, only four kinds of plant states, normal operation, loss of coolant accident (LOCA), steam generator tube rupture (SGTR), and steam line break (SLB) are assumed, and only seven indicators, reactor power, generator power, pressurizer pressure, pressurizer level, steam/feed-water deviation, containment radiation, and secondary radiation, are modeled. Each indicator has three different states, increase, no change and decrease. Therefore,

\[ W = \{\text{normal operation, LOCA, SGTR, SLB}\} \]  

\[ Y_i = \{\text{increase, no change, decrease}\} \quad \text{where } i = 1, 2, \ldots, 7. \]  

When human operators are unaware of the occurrence of the accident, they might think that the plant is in the state of normal operation. However, when they observe the containment radiation high alarm, they might think of the possibility of the occurrence of a LOCA. Therefore, they might actuate the manual reactor trip and safety injection. Fig. 6 shows the generated alarms by CNS for the example situation (the LOCA occurs at 3 min). When human operators are unaware of the occurrence of the accident, they might think that the plant is in the state of normal operation. However, when they observe the containment radiation high alarm, they might think of the possibility of the occurrence of a LOCA. Therefore, they might actuate the manual reactor trip and safety injection.
normal operation. At this time, operators’ understanding of the plant state is assumed to be as follows:

\[ P(X) = \{0.9997, 0.0001, 0.0001, 0.0001\} \]  \hspace{1cm} (12)

At 49 s after the occurrence of the LOCA, human operators will receive containment radiation high alarm, and they observe that the containment radiation is increasing. This observation changes operators’ understanding of the plant state, which can be calculated as shown in (13) using (8). It is shown in Fig. 8 that the Bayesian network model provides an equivalent result.

\[ P(X) = \{0.50055, 0.49935, 0.00005, 0.00005\} \]  \hspace{1cm} (13)

This means that operators consider two possibilities, sensor failure in normal operation or LOCA, with almost equal probabilities. At this moment, it can be said that the failure probability of the manual reactor trip is also about 0.5, as shown in Fig. 8.

If human operators monitor the pressurizer pressure indicators after monitoring the containment radiation indicators, and then observe the pressurizer pressure does not change, due to the CCF of pressurizer pressure sensors, operators’ understanding of the plant state is changed as follows:

\[ P(X) = \{0.999102, 0.000798, 8 \times 10^{-8}, 0.0001\} \]  \hspace{1cm} (14)
If the human operators do not monitor any other indicators, it is highly likely that the human operators understand the situation as the failure of containment radiation sensors in normal operation, and therefore do not actuate manual reactor trip immediately. If the human operators monitor the reactor power indicators after monitoring the pressurizer pressure indicators, it is highly likely that the human operators observe the reactor power is decreasing. But, we have to also consider the possibilities of observing the reactor power does not change or is increasing due to sensor or indicator failures. With the consideration of all these possibilities with corresponding probabilities, operators’ understanding of the plant state changes as follows:

\[ P(X) = \{0.112777, 0.887072, 8.9 \times 10^{-5}, 6.1 \times 10^{-5}\} \]

At this point, the human operators put more belief on the occurrence of a LOCA, and therefore they are more likely to actuate the manual reactor trip. From Eqs. (13)–(15), it can be found that the change in operators’ understanding of the plant state described above well matches with the description of the probable scenario in Section 4.2.

4.4. Consideration of all possible scenarios

The scenario that is described in Sections 4.2 and 4.3 can be summarized with Fig. 9. After observing the increase in the containment radiation, the human operators assess the situation as (13), which is also summarized in Fig. 9. Then, the human operators select the pressurizer pressure indicators and observe that the pressurizer pressure does not change. Based on this observation, they understand the situation as (14), which is also summarized in Fig. 9. But, it cannot be guaranteed that the human operators always monitor the pressurizer pressure indicators after observing that the containment radiation is increasing. What human operators monitor after observing that the containment radiation is increasing has a probability distribution, as shown in Fig. 9. The probabilities are assigned to be proportional to the expected information from each indicator after the observation of the increase in the containment radiation, which can be calculated using (9) [17]. After monitoring an indicator, what the human operators will observe also has a probabilistic distribution, due to the possibilities of sensor or indicator failures. Since there are six indicators and each indicator has three different kinds of states, there are 18 possible observations. The probabilities of the observations are all different, and each observation will produce different indicators’ understanding of the plant state. Table 1 summarizes the 18 different possibilities. It can be seen from Table 1 that the observation of no change in the pressurizer pressure and the resultant operators’ understanding of the plant state is merely one possibility among the 18 possibilities after the observation of the increase in the containment radiation.

Based on the probabilities of the 18 possibilities, their resultant operators’ understanding of the plant state, and corresponding reactor trip failure probabilities, the expected probability distribution for operators’ understanding of the plant state and the expected reactor trip failure probability can be calculated as shown in Table 1. By consecutively conducting similar calculations shown in Table 1, the change of operators’ understanding of plant state and

Fig. 9. Change in operators’ understanding of the plant state after observation of the increase in the containment radiation.
the reactor trip failure probability as the operators monitor more indicators can be calculated. The calculation result is shown in Fig. 10. In Fig. 10, the \(x\)-axis indicates the number of monitored indicators, and the \(y\)-axis indicates the recognized probability of the plant state. It can be seen from Fig. 10 that as operators receive more information, their belief in the occurrence of a LOCA increases, and the failure probability of manual reactor trip decreases.

4.5. Consideration of the effects of context factors

With the proposed framework, we can evaluate the quantitative effects of various context factors to the safety of nuclear power plants, by making quantitative assumptions. Fig. 11 shows a brief summary of the assumptions for the effect of context factors on the process of situation assessment of human operators. The details of the quantitative assumptions are summarized below.

1. The sensor failure probabilities are assumed to be 0.001.
2. Since the adequacy of organization affects the safety culture of the organization, we make quantitative assumption on the safety culture. The assumptions for the four levels of safety cultures are as follows:
   - Very good: Manual actuation of SI when any abnormal situation occurs.
   - Good: Manual actuation of SI when LOCA, SGTR or SLB occurs.
   - Moderate: Manual actuation of SI when LOCA or SGTR occurs.
   - Poor: Manual actuation of SI when LOCA occurs.

### Table 1
Eighteen different possible observations and their resultant operators’ understanding of the plant state after observing that the containment radiation is increasing.

<table>
<thead>
<tr>
<th>Observations</th>
<th>Probability</th>
<th>Normal operation</th>
<th>LOCA</th>
<th>SGTR</th>
<th>SLB</th>
<th>Rx. trip failure probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx. power</td>
<td>Increase</td>
<td>2.5(\times)10^-5</td>
<td>0.333456</td>
<td>0.333256</td>
<td>3.34(\times)10^-5</td>
<td>0.333256</td>
</tr>
<tr>
<td>(p=0.249992)</td>
<td>No change</td>
<td>0.0002</td>
<td>0.999201</td>
<td>0.000799</td>
<td>8.00(\times)10^-8</td>
<td>8.00(\times)10^-8</td>
</tr>
<tr>
<td>Decrease</td>
<td>0.249542</td>
<td>0.0001</td>
<td>0.9998</td>
<td>0.0001</td>
<td>1.00(\times)10^-8</td>
<td>0.000106</td>
</tr>
<tr>
<td>Gen. output</td>
<td>Increase</td>
<td>2.5(\times)10^-5</td>
<td>0.5001</td>
<td>0.4998</td>
<td>5(\times)10^-5</td>
<td>5(\times)10^-5</td>
</tr>
<tr>
<td>(p=0.249842)</td>
<td>No change</td>
<td>0.0002</td>
<td>0.999201</td>
<td>0.000799</td>
<td>8.00(\times)10^-8</td>
<td>8.00(\times)10^-8</td>
</tr>
<tr>
<td>Decrease</td>
<td>0.249392</td>
<td>0.0001</td>
<td>0.9997</td>
<td>0.0001</td>
<td>1.00(\times)10^-8</td>
<td>0.000206</td>
</tr>
<tr>
<td>PRZ press</td>
<td>Increase</td>
<td>0</td>
<td>0.5001</td>
<td>0.4998</td>
<td>5(\times)10^-5</td>
<td>5(\times)10^-5</td>
</tr>
<tr>
<td>(p=0.249842)</td>
<td>No change</td>
<td>0.249617</td>
<td>0.999101</td>
<td>0.000799</td>
<td>8.00(\times)10^-8</td>
<td>9.99(\times)10^-5</td>
</tr>
<tr>
<td>Decrease</td>
<td>0</td>
<td>0.0001</td>
<td>0.9998</td>
<td>0.0001</td>
<td>1.00(\times)10^-8</td>
<td>0.000106</td>
</tr>
<tr>
<td>PRZ level</td>
<td>Increase</td>
<td>2.5(\times)10^-5</td>
<td>0.5001</td>
<td>0.4998</td>
<td>5(\times)10^-5</td>
<td>5(\times)10^-5</td>
</tr>
<tr>
<td>(p=0.249842)</td>
<td>No change</td>
<td>0.0002</td>
<td>0.999101</td>
<td>0.000799</td>
<td>8.00(\times)10^-8</td>
<td>9.99(\times)10^-5</td>
</tr>
<tr>
<td>Decrease</td>
<td>0.249392</td>
<td>0.0001</td>
<td>0.9998</td>
<td>0.0001</td>
<td>1.00(\times)10^-8</td>
<td>0.000106</td>
</tr>
<tr>
<td>STM/FW dev.</td>
<td>Increase</td>
<td>3.19(\times)10^-8</td>
<td>0.250113</td>
<td>0.249862</td>
<td>0.24962</td>
<td>0.24962</td>
</tr>
<tr>
<td>(p=0.000319)</td>
<td>No change</td>
<td>0.000319</td>
<td>0.50015</td>
<td>0.4995</td>
<td>4.00(\times)10^-8</td>
<td>4.00(\times)10^-8</td>
</tr>
<tr>
<td>Decrease</td>
<td>3.19(\times)10^-8</td>
<td>0.5001</td>
<td>0.4998</td>
<td>5(\times)10^-5</td>
<td>5(\times)10^-5</td>
<td>0.50014</td>
</tr>
<tr>
<td>2nd rad. (p=0.000163)</td>
<td>Increase</td>
<td>1.63(\times)10^-8</td>
<td>0.333456</td>
<td>0.333256</td>
<td>0.333256</td>
<td>0.333484</td>
</tr>
<tr>
<td>No change</td>
<td>0.000163</td>
<td>0.500125</td>
<td>0.499825</td>
<td>4.00(\times)10^-8</td>
<td>5(\times)10^-5</td>
<td>0.500165</td>
</tr>
<tr>
<td>Decrease</td>
<td>1.63(\times)10^-8</td>
<td>0.5001</td>
<td>0.4998</td>
<td>5(\times)10^-5</td>
<td>5(\times)10^-5</td>
<td>0.50014</td>
</tr>
<tr>
<td>Average</td>
<td>0.9991</td>
<td>0.250341</td>
<td>0.748626</td>
<td>7.49(\times)10^-5</td>
<td>5.83(\times)10^-5</td>
<td>0.250397</td>
</tr>
</tbody>
</table>
For quantitative analysis, we assume that the safety culture is moderate. 

3. Since the working conditions possibly affects the error probabilities of indicator reading errors, the quantitative assumptions for the three levels of working conditions are as follows:
   - Advantageous: Indicator reading error $Z_{0.0003}$
   - Compatible: Indicator reading error $Z_{0.001}$
   - Incompatible: Indicator reading error $Z_{0.003}$

For quantitative analysis, we assume that the working condition is compatible.

4. Since the adequacy of man–machine interface (MMI) affects the indicator reading time, the quantitative assumptions for the four levels of the adequacy of MMI are as follows:
   - Supportive: Indicator reading time = 5 s
   - Adequate: Indicator reading time = 10 s
   - Tolerable: Indicator reading time = 20 s
   - Inappropriate: Indicator reading time = 40 s

For quantitative analysis, we assume that the working condition is adequate.

5. Since the time of day (circadian rhythm) affects the response time of the human operators, we make the following quantitative assumptions.
   - Day-time (adjusted): (Reading time + Situation assessment time)
   - Night-time (unadjusted): (Reading time + Situation assessment time) $\times 1.5$

For quantitative analysis, we assume that the time of day (circadian rhythm) is day-time (adjusted).

6. Since the adequacy of training is related to the knowledge or expertise of human operators, we make the following quantitative assumptions.
   - Adequate, high experience: know the behavior of all seven indicators
   - Adequate, limited experience: know the behavior of six indicators
   - Inadequate: know the behavior of five indicators

For quantitative analysis, we assume that the adequacy of training is adequate and human operators are highly experienced.

7. Since the crew collaboration quality can affect the verbal communication error probabilities, we make the following quantitative assumptions.
   - Very efficient: Verbal communication error probability $= 0.0003$
   - Efficient: Verbal communication error probability $= 0.001$
   - Inefficient: Verbal communication error probability $= 0.001$
   - Deficient: Verbal communication error probability $= 0.003$

For quantitative analysis, we assume that the crew collaboration quality is efficient.

8. Since the available time affects the stress of human operators, we make quantitative assumptions on...
the stress of human operators. The quantitative assumptions for the four levels of the stress of human operators are as follows:

- Optimal: Inference error probability = 0
- Moderately high: Inference error probability = 0.01
- Very high: Inference error probability = 0.1
- Extremely high: Inference error probability = 0.5

For quantitative analysis, we assume that the stress is optimal.

**Table 2**
Effect of adequacy of organization (safety culture)

<table>
<thead>
<tr>
<th>Adequacy</th>
<th>Very good</th>
<th>Good</th>
<th>Moderate</th>
<th>Poor</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.0009</td>
<td>0.54032</td>
<td>0.067228</td>
<td>0.067304</td>
</tr>
</tbody>
</table>

**Table 3**
Effect of working condition

<table>
<thead>
<tr>
<th>Working Condition</th>
<th>Advantageous</th>
<th>Compatible</th>
<th>Incompatible</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.066813</td>
<td>0.067228</td>
<td>0.068412</td>
</tr>
</tbody>
</table>

**Table 4**
Effect of crew collaboration quality

<table>
<thead>
<tr>
<th>Quality</th>
<th>Very efficient</th>
<th>Efficient</th>
<th>Inefficient</th>
<th>Deficient</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.066813</td>
<td>0.067228</td>
<td>0.067228</td>
<td>0.068412</td>
</tr>
</tbody>
</table>

**Table 5**
Effect of adequacy of procedures

<table>
<thead>
<tr>
<th>Adequacy</th>
<th>Appropriate</th>
<th>Compatible</th>
<th>Inappropriate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.000907018</td>
<td>0.0028025</td>
<td>0.999725</td>
</tr>
</tbody>
</table>

**Table 6**
Effect of stress (available time)

<table>
<thead>
<tr>
<th>Stress Level</th>
<th>Optimal</th>
<th>Moderately high</th>
<th>Very high</th>
<th>Extremely high</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.067228</td>
<td>0.239487</td>
<td>0.299788</td>
<td>0.452516</td>
</tr>
</tbody>
</table>

Based on the quantitative assumptions, the effects of each context factor on the safety of NPPs can be evaluated. Fig. 12 shows the changes of the reactor trip failure probability as functions of time, upon the assumptions of the four levels of the adequacy of organization (safety culture). In Fig. 12, the x-axis indicates the time after the occurrence of the accident, and y-axis indicates the reactor trip failure probability. It can be seen from Fig. 12 that the reactor trip failure probability is lowest when the safety culture is very good and highest when the safety culture is poor. The calculated reactor trip failure probabilities at the time of 150 s upon the assumptions of the four levels of the adequacy of organization (safety culture) are summarized in Table 2. Similarly, from Tables 3–8, the effects of the context factors on the calculated reactor trip failure probabilities are summarized. And, Fig. 13(a) shows the effect of the adequacy of MMI and Fig. 13(b) shows the effects of time of day (circadian rhythm) on the reactor trip failure probability. From this analysis, it can be found that the quantitative effects of the context factors can be estimated in the proposed framework when proper quantitative assumptions are made. In the analysis results shown in from Tables 2–8 and Fig. 13, the adequacy of...
procedure, available time, training/experience of human operators, and sensor failure probabilities are relatively important compared to other factors, in this example situation.

5. Conclusions

It is generally known that the quality of HRA is the bottleneck of the quality of PSA. In this paper, several limitations of current HRA methods are additionally identified such as the lack of considerations on the interdependency between I&C systems and human operators, and lack of theoretical basis for situation assessment. To overcome these limitations, we develop a quantitative safety assessment method for I&C systems and human operators in NPPs with the consideration on the interdependency between I&C systems and human operators. The proposed method includes computational models for the knowledge-driven monitoring of human operators and situation assessment of human operators.

The application of the proposed method to an example situation demonstrates that the quantitative description by the proposed method for a probable scenario well matches with the qualitative description of the scenario. It is also demonstrated that the proposed method can probabilistically consider all possible scenarios and the proposed method can be used to quantitatively evaluate the effects of various context factors on the safety of NPPs. We believe that the proposed method will be particularly useful when the issue of the interdependency of I&C systems and human operators become important, such as for certain special initiating events (e.g., loss of electrical buses) or in fire situations (e.g., causing one or more I&C failures due to affecting multiple cables) in which multiple instrumentation/sensor failures are somewhat likely.

As a result, we expect that the proposed method can be used as the basis for developing advanced quantitative models for probabilistic safety assessment of I&C systems and human operators. With the advanced quantitative models, it is expected that they improve the quality of probabilistic safety assessment (PSA), quantitatively evaluate the effects of instrument faults on the situation assessment of human operators, identify the possibilities of unsafe actions (so-called errors-of-commission) in various situations, and quantitatively evaluate the contribution of various context factors and operator support systems to the increase in the safety of NPPs. In this way, the proposed method is expected to contribute to increase the safety and economy of NPPs in the risk-informed regulation and application environment.

Acknowledgements

This work is partly supported by Korean National Research Laboratory (NRL) program.

References


