Journal of the Korean Nuclear Society
Volume 36, Number 5, pp.430 449, October, 2004

A Quantitative Model of System- Man Interaction Based on Discrete Function Theory

Man Cheol Kim and Poong Hyun Seong
Korean Advanced Institute of Science and Technology
373-1, Guseong-dong, Yuseong-gu, Daejeon, 305-701, Republic of Korea

(Received April 28, 2004)

Abstract

A quantitative model for a control system that integrates human operators, systems, and their interactions is developed based on discrete functions. After identifying the major entities and the key factors that are important to each entity in the control system, a quantitative analysis to estimate the recovery failure probability from an abnormal state is performed. A numerical analysis based on assumed values of related variables shows that this model produces reasonable results. The concept of ' relative sensitivity 'is introduced to identify the major factors affecting the reliability of the control system. The analysis shows that the hardware factor and the design factor of the instrumentation system have the highest relative sensitivities in this model. The probability of human operators performing incorrect actions, along with factors related to human operators, are also found to have high relative sensitivities. This model is applied to an analysis of the TMI-2 nuclear power plant accident and systematically explains how the accident took place.

Key Words : Index Terms-discrete function theory, human operators, man-machine interaction, quantitative model

1. Introduction

Figure 1 shows a block diagram for the control of a plant. In the figure, R(s) indicates the reference input and C(s) indicates the resultant behavior of the plant. Based on Figure 1, it is relatively easy to arrive at the following three propositions for the safe and reliable operation of the plant:

① Design a stable plant
② Design a reliable controller
③ Design a reliable sensor

When human operators are included in the controller shown in Figure 1, the controller forms a control system, which is shown in Figure 2. The sensor in Figure 1 is included in the control system of Figure 2. In Figure 2, the resultant behavior of the plant C(s) and the reference input R(s) are omitted. The control system consists of the following three entities: an instrumentation and control (I&C) system, a man-machine interface

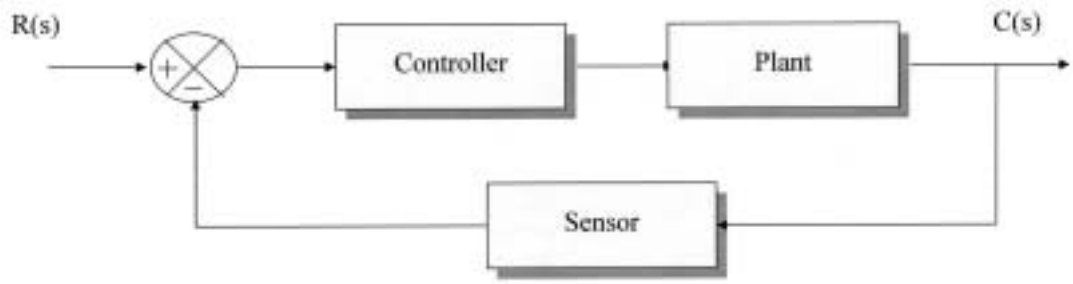

Fig. 1. Block Diagram for the Control of a Plant

(MMI), and human operators.

To design a more reliable control system, many studies have been performed on I&C systems, MMIs, and the behavior of human operators. Among the topics focused on by these studies have been the following: reliability analysis methods for digital systems [1,2], development methods for high-reliability software [3], verification and validation of high - reliability software [4], complexity analysis of the MMI [5], the design of computerized procedures [6], and qualitative and quantitative models for human behavior [7,8,9]. These studies share the same goal, the design of a more reliable control system; however, there have been few discussions concerning the quantitative contribution of such studies to the reliability of the control system (described in Figure 2), as research thus far has generally assessed qualitative contributions.

1.1. The Importance of Quantitative Analysis

A great many components are related in designing a more reliable control system, especially when the control system includes human operators. From the integrity of a small transmission wire to the teamwork of human operators, it would be almost impossible to mention every single component that is related to the control system. In other words, there are innumerable tasks involved in improving the reliability of the control system.

It may be easy to talk about why a specific component is important to a power plant. However, at this point, we believe that it is much more difficult to talk about how a component is important in a power plant. In other words, we can discuss the importance of a specific component in a qualitative way, but not in a quantitative way.

We think that this is mainly because few quantitative models have been developed for the control system, which includes the I&C system, the MMI, and the human operators. Therefore, we believe that it is necessary to establish a quantitative model which takes key factors related to the I&C system, the MMI, and the human operators into account.

1.2. The Objective of Our Research

In this paper, we propose a model for the quantitative analysis of the control system, which includes the I&C system, the MMI, and the human operators. Even though fault tree analyses have successfully served as a general method for quantitative analysis for decades, the fact that such analyses only represent two kinds of system states, success and failure, imposes limitations on the range of their applications, especially with

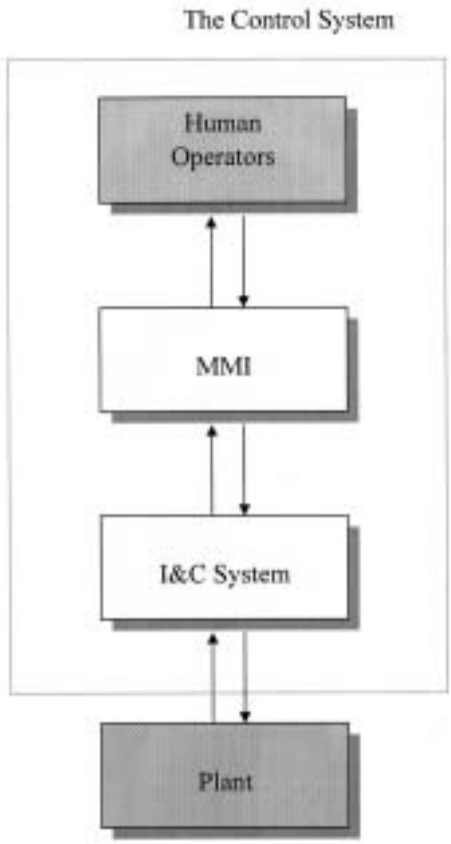

Fig. 2. The Control System Including Human Operators

regard to modeling the errors-of-commission by human operators. We introduce a new method for the quantitative analysis based on discrete functions, which is explained in section III.

2. Identification of Subsystems and Key Factors

2.1. Identification of Subsystems in the I&C System and the MMI

As shown in Figure 2, the I&C system gathers information from the plant and transfers that information to the MMI, while taking some control and protection actions over the plant. The MMI receives information from the I&C system, processes it into a form that human operators can understand, and then transfers the information to the human operators. The human operators receive the information from the MMI and take the role of supervising and controlling the plant.

Based on their functions, the I&C system and the MMI can be divided into smaller subsystems. The I&C system is divided into two subsystems, an instrumentation system and a control/protection system. The instrumentation system performs the

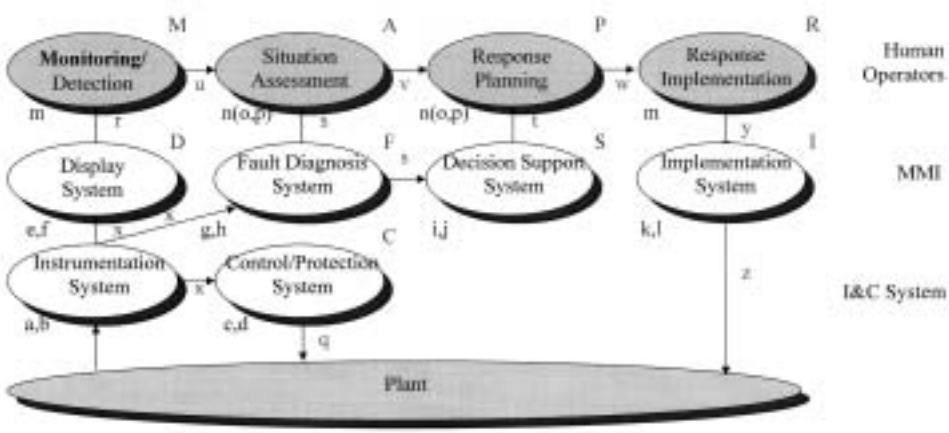

Fig. 3. Basic Configuration of the Proposed Model

function of receiving information from the plant and transferring the information to other systems. It corresponds to the sensor in Figure 1. The control/protection system receives information from the instrumentation system and performs the function of automatic control and protection of the plant.

The MMI, which conceptually includes operator support systems, is divided into the following four subsystems: a display system, a fault diagnosis system, a decision support system, and an implementation system. As will be shown below, the division of the MMI corresponds somewhat to the major cognitive activities of the human operators.

Figure 3 is a detailed version of Figure 2, and it summarizes the division of the I&C system and the MMI, and the information flow among the subsystems. Figure 3 also shows the division of the behavior of human operators, which is explained below.

2.2.Major Cognitive Activities Underlying Human Operator Performance

When considering the behavior of human operators, two kinds of human errors should be considered: errors of omission and errors of commission. ' errors of omission 'are failures to perform required actions, whereas ' errors of commission 'mean performing unnecessary actions that usually worsen a given situation.

Besides the errors that human operators make, the recovery of information also has to be considered. Here, the recovery of information means the ability of human operators to extract or deduce correct information even though such information is not available or the human operators receive incorrect information. For example, even though there is no water level indicator for the reactor in a nuclear power plant, the operators of the plant can deduce the fact that the reactor is filled with water, based on the water level of the pressurizer.

Many human reliability models and human cognitive models have been proposed. However, human reliability models have a strong tendency to consider only errors of omission, overlooking errors of commission and the recovery of information. To consider all the aspects of human behavior stated above, we choose the four major cognitive activities underlying operator performance used in ATHEANA (A Technique for Human Event Analysis) [8,10]. The four major cognitive activities are monitoring/detection, situation assessment, response planning, and response implementation. The four major cognitive activities and related information flow are summarized in Figure 3.

2.3. Overview of the Proposed Model

Figure 3 shows an overview of the proposed model. The nodes in this figure represent the subsystems of the I&C system and of the MMI and the major cognitive activities of human operators. The arrows represent the information flow in the proposed model.

In Figure 3, the instrumentation system receives information from the plant and transfers the received information to other systems, the control/protection system, the display system, and the fault diagnosis system. The control/protection system receives information from the instrumentation system and performs automatic control and protection functions on the plant. The display system receives information from the instrumentation system, and gives the information to human operators in a form that human operators can effectively accept. Human operators receive the information through monitoring/detection activity, and perform situation

assessment with the assistance of the fault diagnosis system. Then, the human operators perform response planning with the assistance of the decision support system. Finally, the prepared responses are implemented (response implementation) through the implementation system.

What is special about this model is the emphasis on the human operators. Human operators take the role of supervising the plant, and make the final decisions in a plant. Because of this important position of human operators, a great deal of research has been conducted to develop qualitative and quantitative models for human operators. However, it seems that the results and recommendations of those studies have not been well integrated in the quantitative analysis of control systems in which human operators are involved. In fault tree analysis, which is the most widely used method for quantitative analysis, human operators are usually treated as a basic event. The basic event usually takes the form of ' operator fails to perform a required action ', with some unavailability value, say 5×10^{-2}. Because a fault tree is a graphical representation of fault propagation in a system, while the qualitative and quantitative models for human operators usually have only a slight relation with the fault propagation, it is not easy to integrate the models into the fault tree analysis.

Also of importance is that a fault tree analysis usually considers only human operators 'failures to perform required actions (i.e., errors-of-omission). However, it has been stated that " human performance problems identified in real operational events often involve operators performing actions which are not required for accident response and, in fact, worsen the plant ' condition (i.e., errors of commission) " [10]. Because fault trees focus on the analysis of the hardware in a system, human operators 'errors-of-commission are not easily expressed in fault trees. However, the proposed model, which focuses on the behavior of human operators, can easily express errors-of-commission, as well as errors-of-omission.

2.4. Key Factors in the Subsystems of the I&C System and the MMI

For the analysis of the proposed model, an overview of which is depicted in Figure 3, key factors related to the nodes (i.e. the subsystems of the I&C system and of the MMI, and the major cognitive activities in human operators) must be identified. We recognize that the characteristics of the subsystems of the I&C system and of the MMI and of the major cognitive activities in human operators are completely different. Therefore, we treat the two categories differently.

The instrumentation system, control/protection system, display system, fault diagnosis system, decision support system, and implementation system are the subsystems of the I&C system and the MMI. Even though they are different in shape,

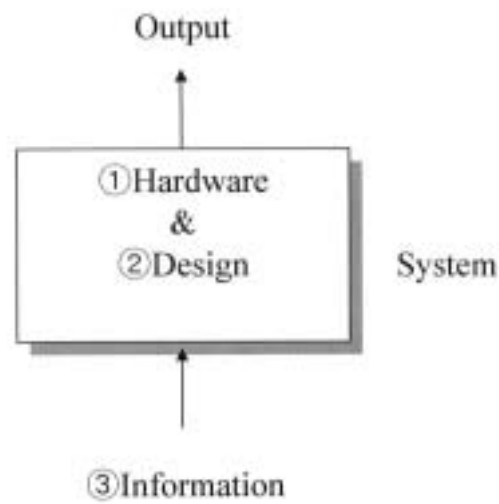

Fig. 4. Conceptual Configuration of a System

functions, etc., all these subsystems commonly belong to the category "system".

Figure 4 shows our way of understanding the conceptual configuration of a system. A system is referred to as a group of independent but interrelated elements comprising a unified whole to perform functions that a single element cannot perform alone. Usually, a system receives information from its previous systems, uses algorithms and hardware to process the information, and then transfers the output to other systems. Therefore, to evaluate whether a system performs its intended functions correctly, the following three factors need to be considered: hardware, design, and information. Hardware refers to the instruments, transmitters, cards, and boards in the system, whereas design refers to the algorithms and software implemented in the system. These two factors, hardware and design, are directly related to the system under consideration. On the other hand, information refers to the received signals, indications and parameters that were originally the outputs of its previous systems. Therefore, information is related to the previous systems, rather than to the system under consideration.

Because the subsystems of the I&C system and the MMI follow the characteristics of the system described in Figure 4, the three factors (hardware, information, and design) commonly become the key factors for the subsystems. In Figure 3, the letters below left of each subsystem of the I&C system or the MMI represent the hardware factor and the design factor of the system, respectively. Letters near arrows represent the information factors to the subsystems, which originally were the outputs of their previous systems. For example, for the control/protection system, the letters *c* and *d* represent the hardware factor and the design factor of the subsystem, respectively, the letter x on the incoming arrow represents the information factor of the subsystem, which originally was the output of the instrumentation system.

2.5. Key Factors in the Major Cognitive Activities of Human Operators

The four major cognitive activities of human operators behave similarly to the subsystems of the I&C system and the MMI. A cognitive activity receives information from a subsystem of the MMI or its previous cognitive activity, processes the information, and then transfers the output to the following subsequent cognitive activity or implementation system (in case the cognitive activity is response implementation). The internal factors (the factors directly related to the cognitive activity under consideration) of each cognitive activity depend on the characteristics of the cognitive activity. In the proposed model, two cognitive activities, monitoring/detection and response implementation, are relatively simple activities, whereas the other two cognitive activities, situation assessment and response planning, are relatively complex activities that require the knowledge, experience, and decision making of human operators.

Based on this consideration, for monitoring/detection and response implementation, simple 'slip error' is considered to be the most important factor, whereas for situation assessment and response planning, "operator ability" is considered to be the most important factor. In Figure 3, the letter *m* below left of monitoring/detection and response implementation represents the "slip error" factor, whereas *n*, below left of situation assessment and response planning, represents the "operator ability" factor.

After comparing three human reliability analysis (HRA) methods, ASEP, ATHEANA, and CREAM, we found that the two factors, available time (or

time stress), training/practice are important in the diagnosis and the execution of a plan by human operators. [11] Therefore, we assume that the operators' ability is mostly affected by two factors: the knowledge (or experience) and the workload (or stress) of human operators. The parentheses beside the factor *n* in Figure 3 mean that the "operator ability" factor is a function of two other factors, *o* and *p*. In Figure 3, and *p* represent the knowledge (or experience) and the workload (or stress) of human operators, respectively. The knowledge (or experience) and the workload (or stress) are categorized into three groups, high (which is denoted as subscript *H*), medium (which is denoted as subscript *M*) and low (which is denoted as subscript *L*). Similarly, other factors can be derived from more elementary factors. It means that a factor in the proposed model is not like a basic event in a fault tree, but rather like a gate in a fault tree that can be expanded to form a tree or network structure. This implies the expansibility of the proposed model. When combined with discrete functions, which will be explained in section III, the proposed model becomes more powerful than existing methods, such as a fault tree analysis or a reliability block diagram, in the analysis of the control system described in Figure 2.

3. Quantitative Analysis Based on Discrete Function Theory

In this section we describe the method that we use for the quantitative analysis of the proposed model. For quantitative analysis, several methods, such as reliability block diagrams, Markov chains, fault tree analysis and Monte Carlo simulation, have been widely used. These methods have various advantages and disadvantages, which are briefly summarized in [12]. Among these methods, fault tree analysis is the most widely used method, due to its applicability to complex systems.

Despite its widespread use, fault tree analysis has several limitations, including the inability to calculate the transient response of a system, the inability to express sequential dependencies, and the inability to express multi-states (more than two states). The method's inability to express sequential dependencies is considered to have been nearly overcome by the work of Dugan et al. [13] (the development of the dynamic fault tree analysis). Among the remaining limitations, we consider the inability to express multi-states to be one of the most critical limitations.

For the quantitative analysis of the proposed model, we propose a method based on the discrete function theory, which is mainly inspired by the work of Choi and Seong [14]. In fact, we do not believe that the method we propose here is completely new. We think that the method is simply not well known and not widely used in the field of quantitative analysis.

3.1. Three States of the Output of a System and the Three Key Factors

In fault tree analysis, the output of a system is regarded as a success or a failure, based on whether a given system performs its intended

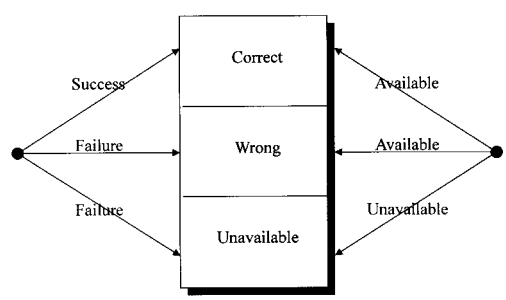

Fig. 5. Three States of the Output of a System

functions and produces the appropriate outputs. This perspective is useful, but there are other aspects that should be considered. From another perspective, the output of a system is regarded as available or unavailable, based on whether the system is physically operational and whether it produces any outputs. When combining these two sperspectives, the output of a system is assumed to be in one of the following three states: correct (available and success), wrong (available but failure), or unavailable. Figure 5 describes how the combination is accomplished.

Systems are not the only category that has these three states. The system hardware, which is one of the three key factors that determine the output of the system, can be operational (available) and produce proper outputs, and thus be in the a ‘ correct ’ state. However, system hardware can also be operational but produce inappropriate outputs because of unrecognized problems, such as drift in resistance or capacitance in electrical components in the hardware, and thus be in a ‘ wrong ’ state. Or, the hardware can be in an ‘ unavailable ’ state. Like the hardware, the other two factors, information and design, can be in one of the three states above.

In summary, the output of a system and the three key factors (hardware, design, and information) commonly can be described to be as being in one of the three states: correct, wrong, or unavailable.

3.2. The Necessity of Multi-States (More than Two States)

Before further description, we think that it is necessary to address why multi-states (more than two states) are needed for describing systems. Rather than giving a lengthy explanation, the following provides a simple illustration. For the analysis of the proposed model, we choose the three states, correct, wrong, and unavailable. The fault tree analysis makes no distinction between the wrong state and the unavailable state. However, we believe that there is a great difference between these two states. If a problem occurs in a system, the information from the system should be discarded. In other words, the system should be put in the unavailable state. But, if the human operators do not recognize the problem and incorrect information, then the human operators will make incorrect control actions. In summary, a system in the wrong state is much more dangerous than a system in the unavailable state, but the fault tree analysis cannot recognize the difference between the two states.

Besides the example above, a much more detailed description of the behavior of the control system would be possible if the quantitative analysis were based on discrete functions, which would allow a description of multi-states in the analysis. However, the use of discrete functions does not necessarily mean that the analysis becomes significantly more complex. Because the fault tree analysis is a special case of the quantitative analysis based on discrete functions, the analysis can be as simple as the fault tree analysis when discrete functions use only two states.

3.3. Discrete Functions

For the system shown in Figure 4, the output of the system is a function of the three key factors (hardware, information, and design), and the output of the system and the three key factors are commonly in one of the three states (correct, wrong, and unavailable). Here, the information refers to all kinds of signals from one entity to other entities.The function can be described mathematically, as follows:

$$f : S^3 \rightarrow S \qquad (1)$$

where the set $\boldsymbol{S}$ = {correct, wrong, unavailable}.

This kind of function is called a discrete function. A discrete function is defined as a function that defines a one-to-one mapping of a domain set which is finite and non-empty, onto a finite non-empty set [15]. In (1), it can be seen that two sets $\boldsymbol{S}$ and $\boldsymbol{S^3}$ are finite non-empty sets, because set S has only 3 elements and set $\boldsymbol{S^3}$ has 27 elements.

A discrete function can be described by a Veitch chart, a well-known tabular representation method. As an example, the Veitch chart for the control/protection system is given in Table I. The behavior of the control/protection system is assumed to be as follows:

- The output of the system is ' correct 'when all three key factors are in the ' correct 'state.
- If at least one factor is in the ' unavailable ' state, the output of the system is ' unavailable '
- If no factors are in the ' unavailable ' state, and at least one factor is in the wrong state, the output of the system is ' Wrong '.

As shown in Table I, there are three key factors (hardware, information, and design) and each key factor is in one of the three states (correct, wrong and unavailable). There are a total of 27 possible cases. For each case, proper output of the function, which is actually the output of the control/protection system, is determined. For example, according to Table I, if the hardware of the control/protection system is in the ' Correct ' state, the information is in the ' wrong 'state and the design is in the ' unavailable 'state, the output of the control/protection system becomes ' unavailable '.

In Veitch charts, a probabilistic approach can be combined. For given probabilities of the three states of the three key factors, the occurrence probabilities of the 27 overall cases can be calculated. Based on the calculation results, the state probabilities of the outputs of the control/protection system can be calculated according to the following equations.

$$P[\text{correct}] = x_C c_C d_C \tag{2}$$

$$P[\text{wrong}] = x_C(c_W d_C + c_C d_W + c_W d_W) + x_W(c_C + c_W)(d_C + d_W) \tag{3}$$

$$P[\text{unavailable}] = x_U + d_U(x_C + x_W) + c_U(x_C + x_W)(d_C + d_W) \tag{4}$$

where the variables c and d denote the hardware and the design factor of the control/protection system, respectively, and the subscripts C, W, and U indicate correct, wrong, and unavailable states, respectively (for example, c_W is the probability that the hardware of the control/protection system is in a wrong state).

3.4. Evaluation I

To illustrate the evaluation of the proposed model, the quantitative analysis of which is based on the discrete function theory, we first describe the evaluation of the control/protection system as an example. Following this example, the evaluation is generalized to other subsystems of the I&C system and of the MMI and the major cognitive activities of human operators. Finally, an evaluation of the overall model will be described.

The evaluation of the control/protection system begins with the construction of the Veitch chart for the system, which is already given in Table I. The Veitch chart is constructed based on the behavior of the control/protection system. The state probabilities of the output of the control/protection system can be calculated according to (2)-(4), but it is convenient to use vector and matrix notations when the analysis is performed for a complex system.

Based on Table I, a probability table for the

control/protection system, shown in Table II, can be constructed. Table II shows the conditional probabilities of the output being in the correct, wrong, or unavailable states, under the conditions that the information is in the correct, wrong, or unavailable states. The conditional probabilities in the table are:

$$c_{CC} = c_C d_C \tag{5}$$

$$c_{CW} = c_W d_C + c_C d_W + c_W d_W \tag{6}$$

$$c_{CU} = d_U + c_U(d_C + d_W) \tag{7}$$

$$c_{WW} = c_C d_C + c_W d_C + c_C d_W + c_W d_W \tag{8}$$

$$c_{WU} = d_U + c_U(d_C + d_W) \tag{9}$$

Table II can be considered as a 3×3 matrix. The matrix is denoted as $\boldsymbol{C}$, as shown in the upper right part of control/protection system in Figure 3. The vector for the state probabilities of the output of the control/protection system is denoted as $\vec{q}$, as shown in Figure 3. The vector , $\vec{q}$ is expressed mathematically, as follows:

$$\vec{q} = \begin{bmatrix} P[correct] \\ P[wrong] \\ P[unavailable] \end{bmatrix}. \tag{10}$$

Because the matrix $\boldsymbol{C}$, which originally comes from Table II, is defined as the conditional probabilities stated above, it is not difficult to prove the following equation.

$$\vec{q} = C\vec{x} \tag{11}$$

It will be convenient to define a function $\boldsymbol{g}$, which takes 2 vectors as input and produces a 3×3 matrix as output, as follows:

$$g(\vec{\alpha},\vec{\beta}) = \begin{bmatrix} \alpha_C\beta_C & 0 & 0 \\ \alpha_W\beta_C + \alpha_C\beta_W + \alpha_W\beta_W & (\alpha_C + \alpha_W)(\beta_C + \beta_W) & 0 \\ \beta_U + \alpha_U(\beta_C + \beta_W) & \beta_U + \alpha_U(\beta_C + \beta_W) & 1 \end{bmatrix} \tag{12}$$

where

$$\vec{\alpha} = \begin{bmatrix} \alpha_C \\ \alpha_W \\ \alpha_U \end{bmatrix} \text{ and } \vec{\beta} = \begin{bmatrix} \beta_C \\ \beta_W \\ \beta_U \end{bmatrix}.$$

This function can be applied to the control/protection system, the display system, the fault diagnosis system, the decision support system, and the implementation system. The following matrixes, shown in Figure 3, can be calculated in a unified way using the function $\boldsymbol{g}$.

$$I = g(\vec{k},\vec{l}) \tag{13}$$

$$S = g(\vec{i},\vec{j}) \tag{14}$$

$$F = g(\vec{g},\vec{h}) \tag{15}$$

$$D = g(\vec{e},\vec{f}) \tag{16}$$

$$C = g(\vec{c},\vec{d}) \tag{17}$$

Then, the following vectors, also shown in Figure 3, can be calculated using the above matrixes.

$$\vec{z} = I\vec{y} \tag{18}$$

$$\vec{z} = I\vec{y} \tag{19}$$

$$\vec{t} = S\vec{s} \tag{20}$$

$$\vec{s} = F\vec{x} \quad (21)$$

$$\vec{q} = C\vec{x} \quad (22)$$

For other subsystems of the I&C system and of the MMI and the major cognitive activities of human operators, the vector for the state probabilities of the output can be calculated in similar ways. Table III summarizes the three key factors and the notations for the factors, the matrixes, and the outputs of the subsystems of the I&C system and the MMI. Similarly, Table IV summarizes the related factors and the notations for the factors, the matrixes, and the outputs of the four major cognitive activities of human operators. As stated above, Figure 3 also summarizes the notations for the factors, the matrixes, and the information flow in the proposed model.

3.5. The Quantitative Analysis for the Proposed Model

When the state probabilities of the factors in Table III and Table IV are determined, the quantitative analysis for the proposed model may begin. As shown in Figure 3, there are two kinds of control actions in the proposed model, $\vec{q}$ and $\vec{z}$, which represent the control actions from the control/protection system and the control actions from human operators, respectively. The combination of these two kinds of control actions is used in the operation of a plant.

In normal operation, the operation of a plant mostly depends on the automatic control of the control/protection system, and human operators are not heavily involved. In this situation, the output of the quantitative analysis depends too much on the factors of the instrumentation system and control/protection system. This is actually outside our interest, and thus we do not apply the proposed model to the normal operation situation.

However, in an abnormal situation, human operators, as well as the subsystems of the I&C system and the MMI, are heavily involved in the operation of the plant. In this situation, human operators and the subsystems of the I&C system and the MMI have to interact with one another to restore the operation situation to normal or to safely shut the plant down. The quantitative

Table I. Veitch Chart with Probabilities for Control/Protection System

	Hardware	C (correct) (c_C)			W (wrong) (c_W)			U (unavailable) (c_U)		
	Design	C (d_C)	W (d_W)	U (d_U)	C (d_C)	W (d_W)	U (d_U)	C (d_C)	W (d_W)	U (d_U)
Information	C (x_C)	C $x_C c_C d_C$	W $x_C c_C d_W$	U $x_C c_C d_U$	W $x_C c_W d_C$	W $x_C c_W d_W$	U $x_C c_W d_U$	U $x_C c_U d_C$	U $x_C c_U d_W$	U $x_C c_U d_U$
	W (x_W)	W $x_W c_C d_C$	W $x_W c_C d_W$	U $x_W c_C d_U$	W $x_W c_W d_C$	W $x_W c_W d_W$	U $x_W c_W d_U$	U $x_W c_U d_C$	U $x_W c_U d_W$	U $x_W c_U d_U$
	U (x_U)	U $x_U c_C d_C$	U $x_U c_C d_W$	U $x_U c_C d_U$	U $x_U c_W d_C$	U $x_U c_W d_W$	U $x_U c_W d_U$	U $x_U c_U d_C$	U $x_U c_U d_W$	U $x_U c_U d_U$

analysis in this paper is performed on the calculation of the probability that the control system in Figure 2 fails to recover the plant from an abnormal situation.

3.6. Evaluation II

When an abnormal situation occurs in a power plant, human operators have to analyze the situation and take the proper control actions. When human operators perform control actions, the control actions by the control/protection system are blocked. Therefore, the recovery of the plant from an abnormal state is solely determined by the control actions of the human operators, which may be in either the correct or the wrong state. In other words, if the control actions of human operators are in the correct state, recovery of the plant will be successful, whereas if the control actions of human operators are in the wrong state, recovery of the plant will fail. If the control actions from human operators are in the unavailable state, recovery of the plant depends on the control actions from the control/protection

Table II. Probability Table forControl/Protection System

Output \ Information	Correct	Wrong	Unavailable
Correct	c_{CC}	*0*	*0*
Wrong	c_{CW}	c_{WW}	*0*
Unavailable	c_{CU}	c_{WU}	*1*

Table III. The Factors and Notations for the Subsystems of I&C System and MMI

	Information	Hardware	Design	Notation for Matrix	Output
Instrumentation System		a_C, a_W, a_U	b_C, b_W, b_U		x_C, x_W, x_U
Control/Protection System	x_C, x_W, x_U	c_C, c_W, c_U	d_C, d_W, d_U	C	q_C, q_W, q_U
Display System	x_C, x_W, x_U	e_C, e_W, e_U	f_C, f_W, f_U	D	r_C, r_W, r_U
Fault Diagnosis System	x_C, x_W, x_U	g_C, g_W, g_U	h_C, h_W, h_U	F	s_C, s_W, s_U
Decision Support System	s_C, s_W, s_U	i_C, i_W, i_U	j_C, j_W, j_U	S	t_C, t_W, t_U
Implementation System	y_C, y_W, y_U	k_C, k_W, k_U	l_C, l_W, l_U	I	z_C, z_W, z_U

Table IV. The Factors and Notations for the Major Cognitive Activities of Human Operators

	Information	Hardware	Design	Notation for Matrix	Output
Monitoring/Detection	Display Sys. (r_C, r_W, r_U)	Slip error (m_C, m_W, m_U)		M	u_C, u_W, u_U
Situation Assessment	Monitoring/ Detection (u_C, u_W, u_U)	Fault Diagnosis Sys. (s_C, s_W, s_U)	Operators' Ability (n_C, n_W, n_U)	A	v_C, v_W, v_U
Response Planning	Situation Assessment (v_C, v_W, v_U)	Decision Support Sys. (t_C, t_W, t_U)	Operators' Ability (n_C, n_W, n_U)	R	w_C, w_W, w_U
Response Implementation	Response Planning (w_C, w_W, w_U)	Slip error (u_C, u_W, u_U)		I	y_C, y_W, y_U

Table V. Eitch Chart with Probabilities for Recovery Failure Probability

Human Response / Control/ Protection	Correct (z_C)	Wrong (z_W)	Unavailable (z_U)
Correct (r_C)	Success ($z_C r_C$)	Failure ($z_W r_C$)	Success ($z_U r_C$)
Wrong (r_W)	Success ($z_C r_W$)	Failure ($z_W r_W$)	Failure ($z_U r_W$)
Unavailable (r_U)	Success ($z_C r_U$)	Failure ($z_W r_U$)	Failure ($z_U r_U$)

system. Table V shows the Veitch chart for the calculation of the final recovery success probability and the final recovery failure probability, Table V can be described mathematically, as follows:

$$\begin{bmatrix} P[success] \\ P[failure] \end{bmatrix} = h(\vec{z}, \vec{q}). \quad (23)$$

One thing that should be noted is that the final recovery failure probability is the sum of the failure rates of errors-of-omission and errors-of-commission. The failure rates of errors-of-omission and errors-of-commission are calculated based on the wrong and unavailable states of the control actions of human operators. Considering the fact that the conventional fault tree analysis method does not consider errors-of-commission, the calculation of the failure rates of errors-of-commission can be one benefit of the proposed method.

3.7. Numerical Analysis

The recovery success probability and recovery failure probability, which can be calculated by (23),

Table VI. The Assumed Values of 30 Variables for Numerical Analysis

Variable	Assumed Value	Variable	Assumed Value	Variable	Assumed Value	Variable	Assumed Value
a_W	α	e_U	α	i_W	α	m_W	0.0001
a_U	α	e_W	α	i_U	α	m_U	0.0001
b_W	α	f_W	α	j_W	α	o_M	γ
b_U	β	f_U	β	j_U	α	o_L	δ
c_W	α	g_W	α	k_W	0.000001	p_H	γ
c_U	α	g_U	α	k_U	0.000001	p_M	δ
d_W	α	h_W	α	l_W	0.000001	-	-
d_U	β	h_U	β	l_U	0.000001	-	-

Table VII. Numerical Results for 9 Cases of Variable Values

		(o_H, o_M, o_L) and (p_L, p_M, p_H).		
		γ=0.1, δ=0.02	γ=0.1, δ=0.01	γ=0.1, δ=0.005
(a_C, a_W, a_U), (b_C, b_W, b_U), (c_C, c_W, c_U), (d_C, d_W, d_U), and so on.	α=0.001, β=0.01	0.999653	0.999674	0.999684
	α=0.0005, β=0.01	0.999744	0.999821	0.999763
	α=0.0001, β=0.01	0.999814	**0.999821**	0.999824

are related to 15 vectors, and thus are functions of 30 variables, because the probability of one state can be calculated if the probabilities of the other two states are given, since the sum of the probabilities of the three states is 1. A numerical analysis is performed to assess the feasibility of the proposed model. The numerical analysis is based on assumed values for the 30 variables.

Among the 30 variables, 24 variables are related to the subsystems of the I&C system and the MMI. Except for the four variables related to the implementation system, 20 variables are divided into two groups, based on the complexities of the related subsystems. The variables in the same group are assumed to have the same value, and the same values for the two groups are denoted as α and β. The division of the variables is summarized in Table VI. As an example, the values of α is assumed to be 10^{-4} and β is assumed to be 10^{-2}. The values of α and βfollow

the unavailability requirement for plant protection systems in nuclear power plants.The implementation system is considered to be very simple compared to other subsystems of the I&C system and the MMI, and thus the probabilities that the hardware factor and the design factor are in the wrong state or in the unavailable state are assumed to be 10^{-6}, as shown in Table VI.

Six variables are related to human operators. The variables related to slip error are assumed to be 10^{-4}, and other factors are divided into two groups, as shown in Table VI. The values for γ is assumed to be 0.1 and δ is assumed to be 0.01.

The recovery failure probabilities for the 9 cases of variable values are summarized in Table VII, where the bold-faced value is the result of the example. The recovery failure probabilities in Table VII show a tendency to decrease when the probabilities of the subsystems of the I&C system and the MMI being in the wrong state or in the

Table VIII. Relative Sensitivities of 30 Related Variables for the Recovery Failure Probability

Variable	Relative Sensitivity ($\times 10^{-6}$)	Variable	Relative Sensitivity ($\times 10^{-6}$)	Variable	Relative Sensitivity ($\times 10^{-6}$)	Variable	Relative Sensitivity ($\times 10^{-6}$)
a_W	**-0.729432**	e_U	-0.157994	i_W	-0.205394	m_W	**-100.046**
a_U	**-0.267943**	e_W	-0.099276	i_U	-0.004087	m_U	-2.14555
b_W	**-0.736727**	f_W	-0.159574	j_W	-0.205394	o_M	**-6.02563**
b_U	**-27.0624**	f_U	-10.0269	j_U	-0.004087	o_L	**-6.16302**
c_W	-0.119049	g_W	-0.452389	k_W	-0.998683	p_H	**-6.16302**
c_U	-0.119049	g_U	-0.0496186	k_U	-0.020362	p_M	**-6.02563**
d_W	-0.120239	h_W	-0.456914	l_W	-0.998683	-	-
d_U	-12.0239	h_U	-5.01152	l_U	-0.020362	-	-

Table IX. Assigned Variable Values for the Analysis of TMI-2 Accident

Variable	Assumed Value	Variable	Assumed Value	Variable	Assumed Value	Variable	Assumed Value
a_W	0.01	e_U	0.01	t_W	0.01	m_W	0.0001
a_U	0.01	e_W	0.01	t_U	0.01	m_U	0.0001
b_W	0.01	f_W	0.01	-	-	o_M	0.3
b_U	0.01	f_U	0.01	-	-	o_L	0.05
c_W	0.01	g_W	0	k_W	0.000001	p_H	0.05
c_U	0.01	g_U	1	k_U	0.000001	p_M	0.3
d_W	0.01	h_W	0	l_W	0.000001	-	
d_U	0.01	h_U	1	l_U	0.000001	-	

unavailable state (α and β) decrease. The recovery failure probabilities in Table VII also show a tendency to decrease when the probabilities of the knowledge of human operators being in the

Table X. Assumed Conditions of TMI-2 and Corresponding Recovery Failure Probability

Plant Condition	Recovery Failure Probability
TMI-2 nuclear power plant	0.0490976
TMI-2 nuclear power plant with well-trained human operators	0.0410904
TMI-2 nuclear power plant with high reliability I&C System and MMI	0.0032576
TMI-2 nuclear power plant with well-trained human operators and high reliability I&C System and MMI	0.0008082

being in the high state (α and β) decrease. While varying according to the values of α, β, γ, and δ the recovery failure probabilities in Table VII seem to be feasible in actual situations.

One thing that should be noted is that the usefulness of the proposed method depends on how easily, reliably, and validly one can estimate the values for the variables. For estimating the values of the variables, we think that the data that is used in the current probabilistic safety assessment (PSA) can be used, with some further analysis. For example, we can obtain the failure probabilities of the plant protection systems. What we have to do is to distinguish the those failures into the failures due to a "wrong" state and failures due to an "unavailable" state. The factors related to human operators can be estimated using the current human reliability analysis (HRA) methods. Even though more efforts necessary to obtain the values of the variables, we believe that the benefits that we can expect from the use of the proposed method can compensate for this additional efforts.

3.8. Relative Sensitivity Analysis

To consider the contribution of each variable to the recovery failure probability, we devise a new concept called relative sensitivity, in contrast to the classical (absolute) sensitivity. The relative sensitivity of the variable x to the function f(x, y, z,...) is defined as follows:

$$\text{Relative Sensitivity} = x \left. \frac{\partial f(x,y,z,\cdots)}{\partial x} \right|_{x=x_1, y=y_1, z=z_1, \cdots} \quad (24)$$

The classical (absolute) sensitivity can be used to evaluate the potential contributions of variables to the function while varying the same "amount" of each variable; whereas the relative sensitivity can be used to evaluate the potential contributions of variables to the function while varying the same "proportion" of each variable. Therefore, if we assume that the same amount of effort is required to decrease the values of variables that have positive sensitivities to the recovery failure probability (i.e. the decrease of the variables decreases the recovery failure probability) by a factor of 10, for example, the relative sensitivity of a variable becomes the direct measure for the effort-effectiveness of the variable for the decrease of the recovery failure probability. Table VIII shows relative sensitivities for 30 variables related to the recovery failure probability in the proposed model, where the bold-faced variables are those that have high relative sensitivities.

The hardware factor and the design factor of the instrumentation system are found to have the highest relative sensitivities in the proposed model. This is because the outputs of all other nodes in the proposed model are dependent on the output of the instrumentation system. According to Table VIII, the probability that human operators perform wrong actions by mistake is also found to have a high relative sensitivity in the proposed model.

This result arises from the fact that, no matter how elaborately the control actions were prepared, if human operators make mistakes while implementing prepared control actions, then, the control system will fail to recover the plant from an abnormal state. The factors related to human operators are also found to have high relative sensitivities in this model, as widely perceived.

4. Accident Analysis

It is widely accepted that an accident is not the result of a single cause. Rather, it is the result of a combination of many complex causes. Certainly, we have to recognize that mechanical and electrical failures in a plant are not unavoidable, no matter how well the plant is designed and constructed, because the properties of hardware degrade naturally. We believe that an important role of the I&C system and human operators (including the MMI) is to provide proper recovery actions when those inevitable mechanical and electrical failures occur somewhere in the plant, as well as to operate and maintain the plant safely.

Therefore, we regard an accident as the failure of a series of those recovery actions. Because the model proposed in this paper is concerned with the evaluation of the success and failure probabilities of the recovery actions, we believe this model can be qualitatively and quantitatively applied to accident analysis.

4.1. The TMI-2 Accident

On Wednesday, March 28, 1979, at 4:00A.M., an abnormal state occurred in the TMI-2 nuclear power plant, located outside of Harrisburg, Pennsylvania, along the Susquehanna River. A valve, that is supposed to be completely closed after automatic operation, remained open because of a mechanical failure. The abnormal state progressed to the point where over 90% of the reactor core was damaged and nearby locations around the plant, as well as the plant itself, were contaminated by radioactivity. The accident, induced by a simple abnormal state, was the most serious commercial nuclear accident in US history. Even though no injuries were reported, the TMI-2 accident precipitated fundamental changes in the way nuclear power plants were operated and regulated. Because of the significance of the TMI-2 accident, we have applied the proposed model to the analysis of this accident.

Before analyzing the history and the sequence of events of the accident, we first need to examine the condition that the plant had been in before the accident. Among a number of problems identified by the Kemeny Commission, which investigated the TMI-2 accident, some of the problems related to the I&C system, the MMI, and the human operators were reported as follows [16]:

- In the TMI-2 nuclear power plant, a large number of control room instruments were out of calibration, and many tags were hanging on the instrument panel indicating equipment out of service. (A problem in the I&C system).
- The TMI-2 control room was not designed with adequate consideration given toward management of an accident: The designers had never systematically evaluated the design to see how well it would serve under emergency conditions. (A problem in the MMI).
- The Kemeny Commission concluded that most of the operators and others involved in the accident did not fully understand the operating principles of the plant equipment. (A problem with human operators).
- Some of the key written operating and emergency procedures in use at TMI were inadequate, including the procedures for a loss-of-coolant accident and for pressurizer operation. (A problem in procedures).

The TMI-2 accident can be characterized as a loss-of-coolant-accident caused by a stuck-open pilot-operated relief valve (PORV) and by the failure of human operators to recognize the malfunction. The sequence of events involved in the initiation of the loss-of-coolant-accident can be summarized as follows:

- The PORV, which had been opened by high pressure, should have been closed when the pressure decreased by a certain amount, but it did not. (A failure in the plant).
- There were no indicators for whether the PORVs were opened or closed. There was an indicator for the command (control) signal of the valve, but not indicating for the actual status of the PORV.
  (A failure of the instrumentation system).
- The operators were faced with over 100 alarms within 10 seconds of the first one. The alarm panel did not give the operators any useful information. (A failure of the display system).
- The operators failed to recognize the occurrence of the loss-of-coolant-accident, despite some critical indications, such as the falling pressure coupled with a constant reactor coolant temperature after the high-pressure injection came on, the high water level alarm signal in the containment building's sump, and a higher than normal count of the neutrons inside the core. (Human error in situation assessment).
- An incorrect situation model used by the operators misled them to reduce the flow rate of high-pressure safety injection. (Human error in response planning).

In applying the proposed model to the TMI-2 accident, the following assumptions are made.

- A fault diagnosis system and a decision support system were not installed at that time.
- The operating and emergency procedures are considered to take the role of the a decision support system. However, the state probabilities of the procedure are not dependant on the information provided by the instrumentation system.

Based on the conditions of the plant before the accident, the values of the variables in the proposed model were assigned as shown in Table IX. According to the assumed variable values for the TMI-2 nuclear power plant, the numerical result for the recovery failure probability can be calculated. The numerical result is:

$$P[failure] = 0.0490976$$
$$\text{(i.e., } P[success] = 0.950902) \qquad (25)$$

Even though the recovery failure probability is two orders higher than that of the example situation given above, the absolute value of the failure probability, 0.049 (one failure of recovery in about 20 plant abnormal conditions), does not seem to be that high. However, when considering the fact that the TMI-2 plant had such a poor history of maintaining equipment, a severe accident seems to have been inevitable.

It would be interesting to determine the recovery failure probability for the TMI-2 nuclear power plant with the assumption that the human operators were well-trained or that a highly reliable I&C system and the MMI were used. The following variable values are used to simulate the assumed conditions, instead of the variable values in Table IX.

① Well-trained operators: $o_M=p_M=0.1$ and $o_L=p_H=0.1$

② High reliability I&C System and MMI : $a_W=a_U=b_W=c_W=c_U=d_W=e_W=e_U=f_W=0.0001$ and, $b_U=d_U=f_U=0.0001$

As shown in Table X, if the human operators of

the plant were well trained, the recovery failure probability decreased slightly. And, if the I&C system and the MMI (even though there was only a display system) were highly reliable, the recovery failure probability decreased by a factor of 15. If these two conditions were satisfied together, the recovery failure probability decreased by a factor of 60.

Therefore, we believe that we cannot place all of the blame on the operators, even though they were actively involved in the accident.

5. Summary and Conclusions

In this paper, we proposed a model for the quantitative analysis of the control system, which consists of the I&C system, the MMI, and human operators. For the quantitative analysis, we introduced a method based on the discrete function theory to represent more than two states in a system, in an effort to overcome the limitations of conventional fault tree analysis. A numerical analysis, which is performed based on assumed variable values, indicates that the model we propose in this paper produces reasonable results.

The concept of ' relative sensitivity ' was devised to identify major factors affecting the recovery failure probability of the control system. The relative sensitivity analysis shows that the hardware factor and design factor of the instrumentation system have the highest relative sensitivities in the proposed model. The probability of human operators performing incorrect actions by mistake also has a high relative sensitivity in the proposed model, as do the factors related to the human operators.

The proposed model is applied to an analysis of the TMI-2 nuclear power plant accident. The quantitative analysis revealed the recovery failure probability from an abnormal state. It was shown that the root cause of the accident was not simply the errors of human operators, but the combination of many failures, because the combination of low operators, ability and low reliability of systems drastically increased the recovery failure probability.

Compared to the fault tree analysis, the model we propose in this paper has a much wider range of applications, because it overcomes one of the most critical limitations of the fault tree analysis, the inability to express multi-states. With more refinement of the proposed model and the data used with it, we believe that the model will become a firm basis both for the quantitative analysis of complex systems, and for the improvement of the safety and reliability of such systems.

Acknowledgements

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

References

1. S. R. Welke, B. W. Johnson and J. H. Aylor, "Reliability Model of Hardware/Software Systems", *IEEE Trans. Reliability*, vol. 44, pp. 413-418, Sep. (1995).
2. K. Vemuri, J. B. Dugan, and K. Sullivan, " Automatic Synthesis of Fault Trees for Computer-Based Systems, " *IEEE Trans. Reliability*, vol. 48, pp. 394-402, Dec.(1999).
3. M. R. Lyu, "An Integrated Approach to Achieving High Software Reliability", *Proc. 1998 IEEE Aerospace Conf.*, vol. 4, pp. 123-136,(1998).
4. H. S. Son and P. H. Seong, "Development of a Safety Critical Software Requirements Verification Method with Combined CPN and PVS: A Nuclear Power Plant Protection

System Application", *Reliab. Eng, Syst. Saf.*, vol.80, pp.19-32, (2003).

5. H. G. Kang and P. H. Seong, "Information Theoretic Approach to Man-Machine Interface Complexity Evaluation", *IEEE Trans. Syst., Man, and Cybern. A*, vol. 31, pp. 163-171, May (2001).
6. Y. Jung, Y. Shin and I. Park, "An incremental objective achievement model in computerized procedure execution", *Reliab. Eng, Syst. Saf.*, vol.70, pp. 185-195, Nov. (2000).
7. A. D. Swain and H. E. Guttmann, *Handbook of Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications Final Report*, NUREG-CR-1278, S.N.L, (1983).
8. U. S. NRC, *Technical Basis andImplementation Guidelines for ATHEANA*, NUREG-1624, (1998).
9. E. Hollnagel, *CREAM : Cognitive Reliability and Error Analysis Method*, New York: Elsevier, (1998).
10. C. M. Thomson et al., "The Application of ATHEANA: A Technique for Slip error Analysis", *Proc. IEEE Sixth Annual Human Factors Meeting*, Orlando, Florida, (1997).
11. M. C. Kim and P. H. Seong, "Incorporating Second Generation Human Reliability Analysis Methods into Current Probabilistic Safety Assessment" Transactions on American Nuclear Society, vol.90, pp.430-431, (2004).
12. M. C. Kim and P. H. Seong, "An Integrated Model For Reliability Estimation of Digital Nuclear Protection System Based on Fault Tree and Software Control Flow Methodologies" *Proc. 4th Japan-Korea Seminar on Advanced Reactors*, Japan, Oct. (2000).
13. J. B. Dugan, S. J. Bavuso, and M. A. Boyd, "Dynamic fault-tree models for fault tolerant computer systems", *IEEE* Trans. *Reliability*, vol. 41, pp. 363-377, Sep. (1992).
14. J. G. Choi and P. H. Seong, "Dependability Assessment of Nuclear Digital Systems using Discrete Function Theory and Fault Injection Experiment", *Reliab. Eng, Syst. Saf.*, submitted for publication, (2004).
15. M. Davio, J. -P. Deschamps and A. Thayse, *Discrete and Switching Functions*, London: Georgi Publishing Company and McGraw-Hill International Book Company, (1978).
16. N. G. Leveson, *Safeware*, New York: Addison-Wesley Publishing Company, (1995).