An Integrated Model for Reactor Control Based on Discrete Function Theory

Man Cheol Kim and 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, Republic of Korea
mckim@nesun1.kaist.ac.kr ; phseong@mail.kaist.ac.kr

ABSTRACT

In this paper, we propose a model for the quantitative analysis of the reactor control system which consists of I&C systems, MMI and human operators. The proposed model is to produce the best quantitative measure for the safety of reactor control based on all available knowledge related to the reactor control. After dividing the I&C systems and MMI into the subsystems and identifying the major cognitive activities of human operators, key factors related to the subsystems and cognitive activities are identified. For the subsystems of the I&C systems and MMI, the three factors, hardware, information and design, are commonly found to be important. For human operators' cognitive activities, simple error, operators' knowledge and workload are found to be important. For the quantitative analysis, we introduce 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. Based on the speculation on the states of a general system and human cognitive activities, the states of the key factors of each subsystem and cognitive activity are determined. Numerical analysis based on assumed values of 30 related parameters in the proposed model shows that the proposed model produces reasonable results.

1. INTRODUCTION

Many researches have been performed in the field of nuclear instrumentation and control (I&C), man-machine interface (MMI) and the behavior of human operators. Even though those researches have their own specific and unique purposes, the ultimate goal of the researches may be the same, to make nuclear power plants *more reliable and safer*.

Therefore, we believe that at this point it is necessary to establish a model which takes all aspects of nuclear I&C systems, MMI and human operators and find out the most critical and important parts on which our future researches and the improvement efforts have to concentrate. With this model, a quantitative analysis of the reliability and the safety of I&C systems including the interaction with human operators seems to be possible.

2. THEORETICAL PRELIMINARIES

System is a group of independent but interrelated elements comprising a unified whole to produce outputs which a single element cannot produce alone. Physically, a system is an assembly of hardware elements. It receives information and processes the information based on the designed algorithms, and then transfers outputs to other systems. Therefore, to evaluate whether a system performs its intended functions correctly or not, the following three factors are needed to be considered, hardware, information and design. In other words, the output of a system can be described as a function of the three main factors.

From one viewpoint, the result of a system is regarded as success or failure. From another viewpoint, the result of a system is regarded as available or unavailable. When combining these two viewpoints, the output of a system is assumed to be in one of the following three states: correct, wrong and unavailable. Not only the system, but also the three main factors mentioned above are expected to be in one of the three states.

In summary, the behavior and the output of a system is a function of three major factors (hardware, information and design), and the system and the three major factors are commonly in one of the three states (correct, wrong and unavailable). In mathematical expression, the function can be described as follows:

$$f : S^3 \rightarrow S \tag{1}$$

where the set ***S***={correct, wrong, unavailable}.

This kind of functions is called discrete functions. 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 another finite non-empty set [1]. In (1), it can be seen that two sets ***S*** and $\boldsymbol{S^3}$ are finite non-empty sets because the set ***S*** has only 3 elements and the set $\boldsymbol{S^3}$ has 27 elements.

The calculation can be performed based on the Veitch chart, a well-known tabular representation method for discrete functions. Table I shows the Veitch chart for typical systems, which is constructed based on the following conditions.

- The system output is ‘correct’ when all three major factors are in the ‘correct’ state.
- If at least one factor is in the ‘unavailable’ state, the system output is ‘unavailable’.
- If no factors are in the ‘unavailable’ state, and at least one factor is in the wrong state, the system output is ‘wrong’.

In the Veitch chart, probabilistic approach can be combined. For given probabilities of the three states of the three major factors, the occurrence of overall 27 cases can be calculated. Based on the calculation results, the state probabilities for typical systems represented in Table I can be calculated as follows:

$$\text{P[correct]} = \alpha_C\, \beta_C \gamma_C \tag{2}$$

$$\text{P[wrong]} = \alpha_C\, (\beta_W \gamma_C + \beta_C\, \gamma_W + \beta_W\, \gamma_W\,) + \alpha_W\, (\beta_C + \beta_W\,)(\gamma_C + \gamma_W) \tag{3}$$

Table I Veitch chart with probabilities for typical systems

	Information	*C (correct)* (α_C)			*W (wrong)* (α_W)			*U (unavailable)* (α_U)		
	Design	*C* (β_C)	*W* (β_W)	*U* (β_U)	*C* (β_C)	*W* (β_W)	*U* (β_U)	*C* (β_C)	*W* (β_W)	*U* (β_U)
Hardware	*C* (γ_C)	C $\alpha_C\beta_C\gamma_C$	W $\alpha_C\beta_W\gamma_C$	U $\alpha_C\beta_U\gamma_C$	W $\alpha_W\beta_C\gamma_C$	W $\alpha_W\beta_W\gamma_C$	U $\alpha_W\beta_U\gamma_C$	U $\alpha_U\beta_C\gamma_C$	U $\alpha_U\beta_W\gamma_C$	U $\alpha_U\beta_U\gamma_C$
	W (γ_W)	W $\alpha_C\beta_C\gamma_W$	W $\alpha_C\beta_W\gamma_W$	U $\alpha_C\beta_U\gamma_W$	W $\alpha_W\beta_C\gamma_W$	W $\alpha_W\beta_W\gamma_W$	U $\alpha_W\beta_U\gamma_W$	U $\alpha_U\beta_C\gamma_W$	U $\alpha_U\beta_W\gamma_W$	U $\alpha_U\beta_U\gamma_W$
	U (γ_U)	U $\alpha_C\beta_C\gamma_U$	U $\alpha_C\beta_W\gamma_U$	U $\alpha_C\beta_U\gamma_U$	U $\alpha_W\beta_C\gamma_U$	U $\alpha_W\beta_W\gamma_U$	U $\alpha_W\beta_U\gamma_U$	U $\alpha_U\beta_C\gamma_U$	U $\alpha_U\beta_W\gamma_U$	U $\alpha_U\beta_U\gamma_U$

$$\text{P[unavailable]} = \alpha_U+\gamma_U\,(\alpha_C+\alpha_W)+\beta_U\,(\alpha_C+\alpha_W)\,(\gamma_C+\gamma_W) \tag{4}$$

3. THE PROPOSED MODEL

Figure 1 shows the basic configuration for the model. The model can be divided into three levels, I&C systems, MMI and human. In Figure 1, ellipses represent the nodes where information processing occurs, and arrows represent the information flow from one node to another. Blue small letters bottom-left of each node denote the major factors related to the node, mostly hardware and design. Green small letters near arrows denote the state probability vectors of the information being transferred. Red capital letter top-right of each node represents a 3×3 matrix which will facilitate the calculation of the node output.

Basically, the model consists of three major entities, I&C systems, MMI and human. I&C systems gather information from the nuclear power plant and transfer the information to MMI while taking some control and protection actions to the plant. The MMI receives information from I&C systems and processes it into the form that human can understand and then transfers the information to human. Human receives information from the MMI and takes the role of supervising and controlling the plant. In this simple model, two entities, human and I&C systems, can take control actions, but by the fact that human can override the control actions taken by I&C systems, human is the final decision maker in this model.

The entity human operators is divided into the four activities, monitoring/detection, situation assessment, response planning and response implementation, based on the four major cognitive activities of nuclear power plant (NPP) operator performance used in ATHEANA (A Technique for Human Event Analysis) [2]. The entity MMI, which conceptually includes operator support systems, is divided into the following four smaller systems, display system, fault diagnosis system, decision support system and implementation system. The division of MMI somewhat corresponds to the four major cognitive activities of human operators. I&C systems are divided into two systems, instrumentation system and control/protection system, according their major functions.

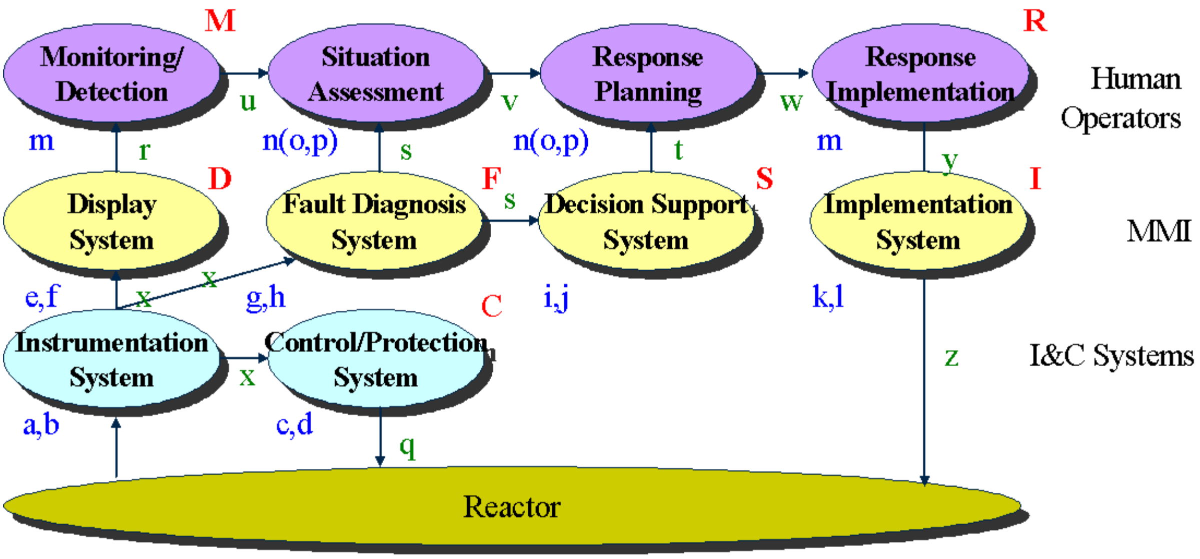


Figure 1 Basic configuration of the model

Table II Probability table for control/protection system

Information Control System	Correct	Wrong	Unavailable
Correct	c_{CC}	*0*	*0*
Wrong	c_{CW}	c_{WW}	*0*
Unavailable	c_{CU}	c_{WU}	*1*

With the framework of the model, the quantitative analysis will be explained below.

3.1 INSTRUMENTATION SYSTEM

For the instrumentation system, the information from the reactor is considered to be always available and correct. Some output from the instrumentation system would be unavailable because it is not included in the design. Some output would be wrong because maybe the way it is monitored is not correct (design fault). If there is a hardware problem in an instrument and the problem is recognized, the corresponding output is considered to be unavailable. If there is an unrecognized hardware problem in an instrument, the corresponding output would be wrong.

Based on the state probabilities of design and hardware nodes in the instrumentation system, the state probabilities of the instrumentation system can be calculated as follows:

$$P[correct] = x_C = a_C b_C \tag{5}$$

$$P[wrong] = x_W = a_C b_W + a_W b_C + a_W b_W \tag{6}$$

$$P[unavailable] = x_U = a_U + b_U(a_C + b_W). \tag{7}$$

3.2 CONTROL/PROTECTION SYSTEM

The role of control/protection system is to receive information from the instrumentation system, whose state probabilities are calculated above, and then take some control and protection actions to the plant. Because control/protection system cannot be perfect, control actions taken by control/protection system can be correct, wrong and unavailable, depending on the states of the three factors, hardware, information and design, of the system. One thing different from the case of the instrumentation system is that in this case information factor is also considered because it receives information from its previous system, the instrumentation system. Here, software faults are considered to be design faults.

Veitch chart with probabilities for the control/protection system can be constructed, which has the same form with that of typical systems shown in Table I. Based on the Veitch chart with probabilities for control/protection system, the probability table shown in Table II can be constructed. The probabilities for each element in the table are:

$$c_{CC} = c_C\, d_C \tag{8}$$

$$c_{CW} = c_W\, d_C + d_C\, d_W + d_W\, d_W \tag{9}$$

$$c_{CU} = c_U + d_U(c_C + d_W) \tag{10}$$

$$c_{WW} = c_C\, d_C + c_W\, d_C + c_C\, d_W + c_W\, d_W \tag{11}$$

$$c_{WU} = c_U + d_U(c_C+c_W) \tag{12}$$

where the variable c and d are related to the hardware and design of the control/protection system respectively and the subscripts C, W and U means correct, wrong and unavailable respectively (for example, c_W means the proportion that the hardware of the control/protection system is in the wrong state). Table II can be considered as a 3×3 matrix, which is denoted as C. The vector for the state probabilities of the control/protection system is denoted as $\vec{q}$ and can be calculated as follows:

$$\vec{q} = C\vec{x} \tag{13}$$

3.3 MAN-MACHINE INTERFACE

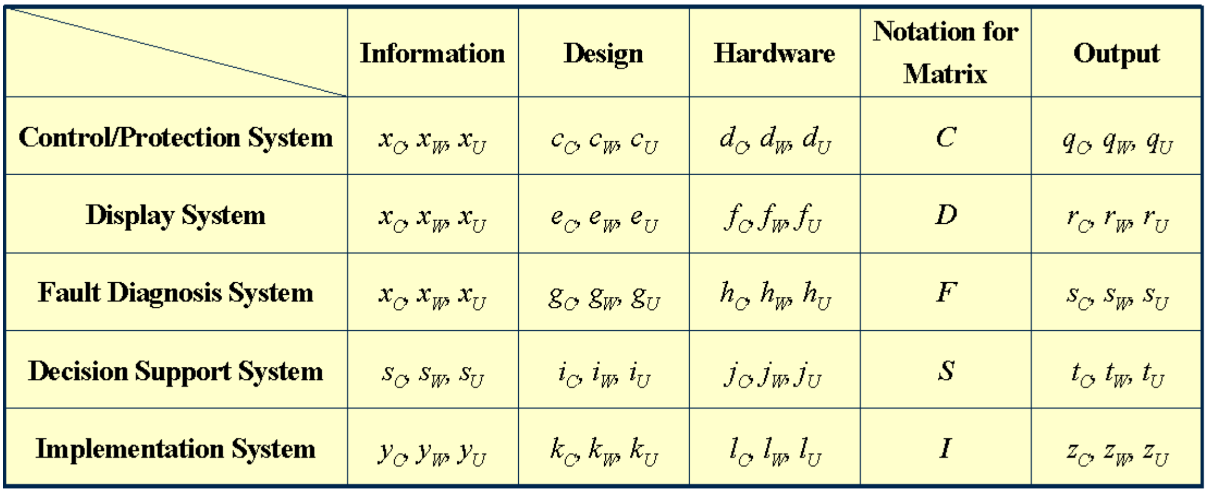
Display system, fault diagnosis system, decision support system and implementation system are subsystems of MMI. Veitch charts for those systems are similar to that of the typical system which was explained in the theoretical preliminaries, as was the control/protection system. Therefore, the calculation procedure applied to the control/protection system can be applied to those systems. Table III shows the comparison of MMI systems to the control/protection system.

3.4 HUMAN

Human behavior is also modeled using discrete functions, but it does not seem to be appropriate to describe human behavior using the three factors, hardware, information and design. For each of the four major cognitive activities shown in Figure 1, other appropriate factors were chosen, which is summarized in Table IV.

Monitoring/Detection is the process in which human operators receive information from MMI and make it their own. This is relatively easy task and maybe considered as the 'skill-based behavior' in the Rasmussen's model of cognitive control. Human operators possibly fail to read some information

Table III Comparison of MMI systems with control/protection system



	Information	Design	Hardware	Notation for Matrix	Output
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

from the display system (unavailable). Or, they possibly read some information incorrectly (wrong). The main cause of this kind of failure is assumed to be simple human error.

Situation Assessment is the process to form situation model, which is human operators' understanding of what situation the plant is in. This stage is the only stage in the model that recovery takes place, i.e. even though monitoring/detection or fault diagnosis system is in the wrong or unavailable state, knowledgeable operators can establish correct situation model via deduction from other related information.

Operators' ability is assumed to be in one of the following three states: high, medium and low. Even though operators' ability is one of the three major factors which determine the output of situation assessment, operators' ability is also assumed to be a function of two other factors related to human operators, expertise and stress (workload per allowed time). The two factors, expertise and stress, are also treated discretely. They also have one of the three state, high, medium and low, as with operators' ability.

Based on the situation model established in the situation assessment process, human operators have to decide what actions to take. This process is called response planning. Response planning is considered to be a function of three factors: situation assessment, decision support system and operators' ability.

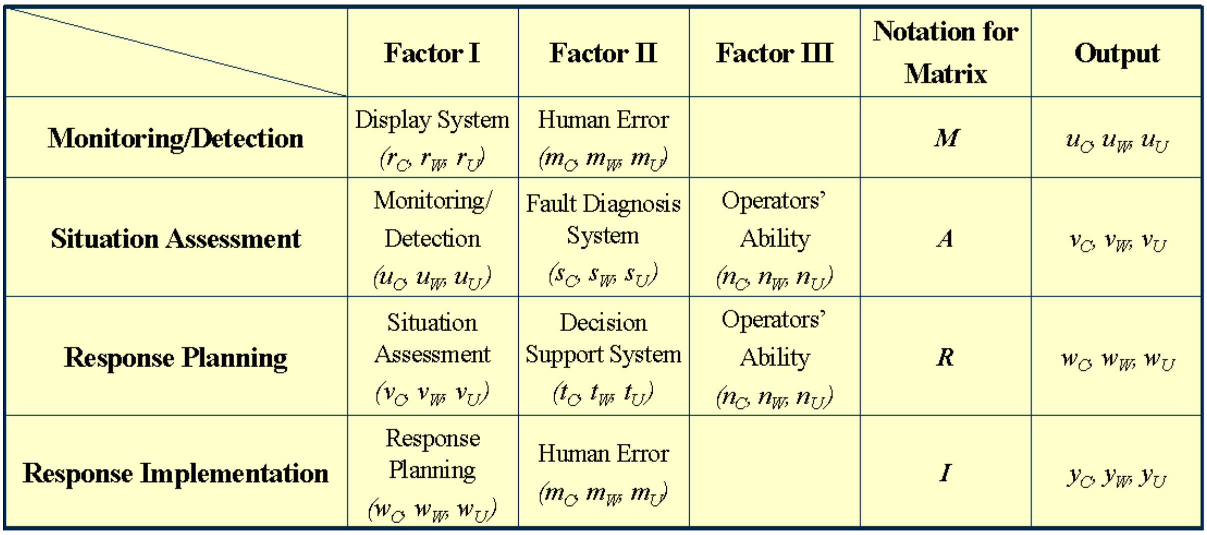
Based on the prepared response in the response planning process, human operators take required actions to the plant. This process is called response implementation. The response implementation is relatively easy task. The factors that affect the response implementation process are response planning and human error.

When human response is implemented, the actions implemented by the control/protection system would be blocked. Based on the state probabilities of human response and control/protection system, the probability that the plant is recovered from an abnormal state can be calculated. Because nuclear power plants are designed to reach hot standby state in an abnormal situation, it seems that 'do nothing' can be a good response because the control/protection systems take some actions according to the algorithms implemented to them.

3.5 EVALUATION

When an abnormal situation occurs, human operators have to analyze the situation and take proper

Table IV Four major cognitive activities in human operators and their related factors



	Factor I	Factor II	Factor III	Notation for Matrix	Output
Monitoring/Detection	Display System (r_C, r_W, r_U)	Human 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 System (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 System (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)	Human Error (m_C, m_W, m_U)		I	y_C, y_W, y_U

control actions to the plant. When human operators take control actions, control actions by the control/protection system are blocked. Therefore, if the control actions of human operators are in the correct or wrong state, the recovery of the plant from an abnormal state is solely determined by the control actions of the human operators. 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 control actions from the control/protection system.

3.6 AN EXAMPLE

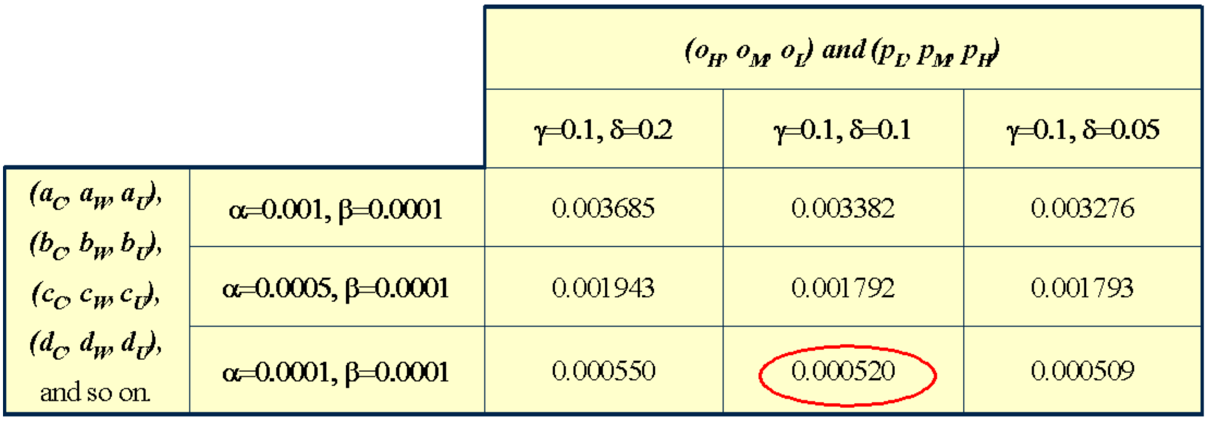
A quantitative analysis is performed for an example which makes the following assumptions:
- The probability that the hardware in various systems belongs to the unavailable state, the probability that the hardware or the design in various systems belongs to the wrong state are commonly assumed to be 10^{-4}, which is denoted as α.
- The probability that the design in various systems belongs to the unavailable state is also assumed to be 10^{-4}, which is denoted as β..
- The implementation system is considered to be extra simple, thus the probabilities of hardware and design to be in the wrong state and the unavailable state are assumed to be 10^{-6}.
- For human operators, the state probabilities of the expertise, stress and human error are assumed to be as follows:

Human Error: P[none]=m_C=0.9998, P[exist]=m_W =0.0001, P[no action]= m_U=0.0001
Expertise : P[high]=o_H= 0.8, P[medium]=o_M=0.1 (γ), P[low]= o_L= 0.1(δ).
Stress : P[high]=p_H =0.1 (δ), P[medium] = p_M = 0.1 (γ), P[low] =p_L = 0.8

where Greek letters indicate that the values are denoted as those Greek letters.
Numerical results for 9 cases of state probabilities are shown in Table VI, where the encircled is the result of the example. By varying α and β the 9 cases were generated. The numerical analysis shows that this model produces reasonable results.

CONCLUSIONS

Table V Recovery failure probabilities for 9 cases of state probabilities



		$(o_H, o_M\ o_L)$ and $(p_L, p_M\ p_H)$		
		γ=0.1, δ=0.2	γ=0.1, δ=0.1	γ=0.1, δ=0.05
$(a_C\ a_W, a_U)$, $(b_C\ b_W, b_U)$, $(c_C\ c_W, c_U)$, $(d_C\ d_W, d_U)$, and so on.	α=0.001, β=0.0001	0.003685	0.003382	0.003276
	α=0.0005, β=0.0001	0.001943	0.001792	0.001793
	α=0.0001, β=0.0001	0.000550	0.000520	0.000509

A quantitative model in which human, systems and their interactions are integrated are developed using discrete functions with the probability concept combined. After identifying the key factors that are important to each entity in the system, numerical analysis is performed according to assumed values of related parameters. The numerical analysis shows that this model produces reasonable results.

REFERENCES

1. M. Davio et al., *Discrete and Switching Functions*, Georgi Publishing Company and McGraw-Hill International Book Company (1978)
2. C. M. Thomson et al., "The Application of ATHEANA: A Technique for Human Error Analysis", *Proceeding of IEEE Sixth Annual Human Factors Meeting*, Orlando, Florida, Vol.9, pp.13-17 (1997)
3. N. G. Leveson, Safeware, Addison-Wesley Publishing Company (1995)