Proceedings of the Korean Nuclear Society Autumn Meeting
Seoul, Korea, October 2001

A Quantitative Model of System Man Interaction Using Discrete Functions

Man Cheol Kim and Poong Hyun Seong

Korea Advanced Institute of Science and Technology
373-1 Kusong-dong, Yusong-gu
Taejon 305-701, Korea

Abstract

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. The concept of 'relative sensitivity' is devised to identify key factors related to the reliability of the system in this model. This model is also applied to the analysis of the TMI-2 accident and reveals that the accident took place because of the combination of the failures in I&C systems, MMI and human operators.

I. 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 which our future researches and the improvement efforts have to concentrate on. 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.

II. Theoretical Preliminaries

System is a group of independent but interrelated elements comprising a unified whole to perform functions 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, ①Hardware, ②Information and ③Design. 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 : ① correct, ②wrong and ③unavailable. Not only the system, but also the three main factors

	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 $\alpha_U\beta_U\gamma_U$

Table 1 Veitch Chart with Probabilities for Typical Systems

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:

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

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 Eq.(1), it can be seen that two sets S and S^3 are finite non-empty sets because the set ***S*** has only 3 elements and the set S^3 has 9 elements.

The calculation can be performed based on the Veitch chart, a well-known tabular representation method for discrete functions. Table 1 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 1 can be calculated as follows:

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

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

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

III. The Proposed Model

Fig.1 shows the basic configuration for the model. The model can be divided into three

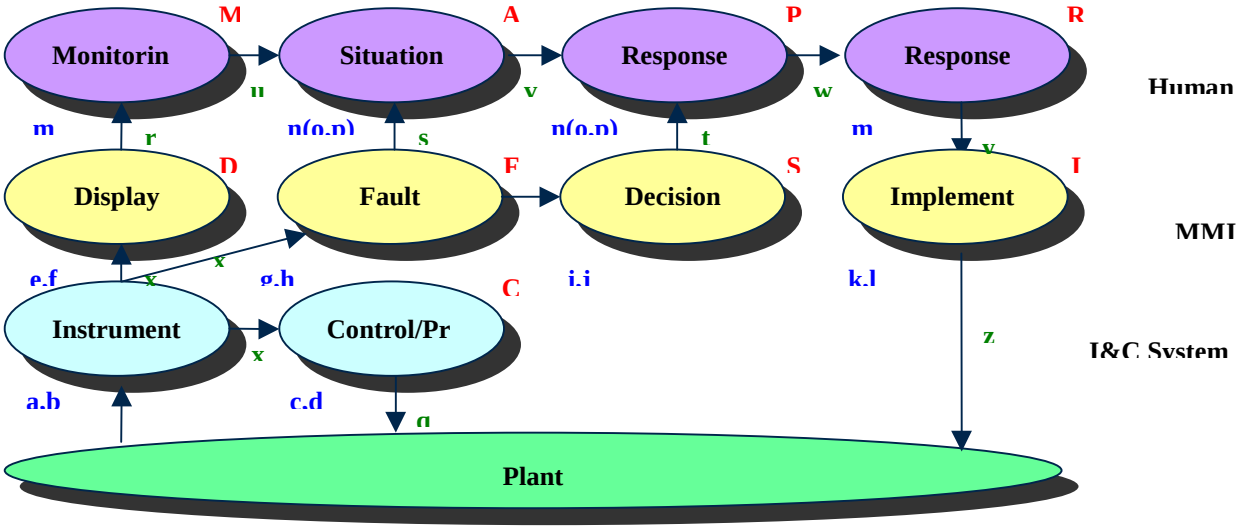

Fig. 1 Basic Configuration for the Model

levels, I&C systems, MMI and human. In Fig. 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 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.

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

Instrumentation System

For the instrumentation system, the information from the plant 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

Design / **Hardware**	Correct (a_C)	*Wrong* (a_W)	*Unavailable* (a_U)
Correct (b_C)	Correct ($a_C b_C$)	Wrong ($a_W b_C$)	Unavailable ($a_U b_C$)
Wrong (b_W)	Wrong ($a_C b_W$)	Wrong ($a_W b_W$)	Unavailable ($a_U b_W$)
Unavailable (b_U)	Unavailable ($a_C b_U$)	Unavailable ($a_W b_U$)	Unavailable ($a_U b_U$)

Table 2 Veitch Chart with Probabilities for Instrumentation System

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

Table 3 The Probability Table for Control/Protection System

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 using the Veitch chart with probabilities shown Table 2.

The calculated state probabilities are:

$P[correct] = x_C = a_C b_C$ $P[wrong] = x_W = a_C b_W + a_W b_C + a_W b_W$ $P[unavailable] = x_U = a_U + b_U(a_C + b_W)$.

The vector for the state probabilities of the instrumentation system is denoted as $\vec{x}$, where

$$\vec{x} = \begin{bmatrix} P[correct] \\ P[wrong] \\ P[unavailable] \end{bmatrix}$$

	Informatio	Design	Hardware	Notation f	Output
Control/Protection	x_C, x_W, x_U	c_C, c_W, c_U	d_C, d_W, d_U	***C***	$q_C, q_W,$
Display System	x_C, x_W, x_U	e_C, e_W, e_U	f_C, f_W, f_U	***D***	$r_C, r_W,$
Fault Diagnosis System	x_C, x_W, x_U	g_C, g_W, g_U	h_C, h_W, h_U	***F***	$s_C, s_W,$
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***	$z_C, z_W,$

Table 4 Comparison of MMI systems with the Control/Protection System

	Factor I	Factor II	Factor III	Notation for Matrix	Output
Monitoring/Detection	Display Sys. (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	Fault Diagnosis Sys.	Operators' Ability	***A***	v_C, v_W, v_U
Response Planning	Situation Assessment	Decision Support Sys.	Operators' Ability	***R***	w_C, w_W, w_U
Response Implementation	Response Planning	Human Error (m_C, m_W, m_U)		***I***	y_C, y_W, y_U

Table 5 Four Major Cognitive Activities in Human and Their Related Factors

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 step system, the instrumentation system. In 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 1.And, based on the Veitch chart with probabilities for control/protection system, the probability table shown in Table 3 can be constructed. The probabilities for each element in the table are:

$$c_{CC} = c_C\, d_C$$
$$c_{CW} = c_W\, d_C + d_C\, d_W + d_W\, d_W$$
$$c_{CU} = c_U + d_U(c_C + d_W)$$
$$c_{WW} = c_C\, d_C + c_W\, d_C + c_C\, d_W + c_W\, d_W$$
$$c_{WU} = c_U + d_U(c_C + c_W)$$

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 3 can be considered as a 3x3 matrix, which is denoted as $\boldsymbol{C}$. The vector for the state probabilities of the control/protection system is denoted as $\vec{q}$ and can be calculated as follows:

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

Man-Machine Interface

Display system, fault diagnosis system, decision support system and implementation system are subsystems of MMI. Those systems 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 4 shows the MMI systems, display system, fault diagnosis system, decision support system and implementation system, with the control/protection system.

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 Fig. 2, other appropriate factors were chosen, which is summarized in Table 5.

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 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 : ①high, ② medium and ③low. 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, ①expertise and ②stress (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 : ①situation assessment, ② decision support system and ③operators' 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

		(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

Table 6 Numerical Results for 9 Cases of State Probabilities

implementation is relatively easy task. The factors that affects the response implementation process are ①response planning and ② 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 status 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. Therefore, the response

Evaluation

The evaluation can be performed using a series of simple matrix multiplication. The final recovery probability is a function of 15 vectors (30 variables) and can be calculated as follows

$$\begin{bmatrix} P[success] \\ P[\ failure] \end{bmatrix} = BZ^{\rho}$$
$$= BIY^{\rho}$$
$$= BIRW^{\rho}$$
$$= BIRPV^{\rho}$$
$$= BIRPAU^{\rho}$$
$$= BIRPAMR^{\varpi}$$
$$= BIRPAMDX^{\rho}$$

An Example

A quantitative analysis is performed for an example which makes the following assumptions:

① 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.

② The probability that the design in various systems belongs to the unavailable state is assumed to be 10^{-2}, which is denoted as β, if the implemented algorithm would be complex, or 10^{-4} if the implemented algorithm seems to be simple

③ 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}.

④ 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= 0.89, P[medium]=o_M=0.1 (γ), P[low]= o_L= 0.01(δ).
Stress : P[high]=p_H =0.01 (δ), P[medium] = p_M = 0.1 (γ), P[low] =p_L = 0.89

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 6, where the encircled is the result of the example. By varying α and δ, the 9 cases were generated. The numerical analysis shows that this model produces reasonable results.

Relative Sensitivity Analysis

To take the contribution of each parameter to the probability of recovery success into account, we devise a new concept named 'relative sensitivity', in contrast to the classical ("absolute") sensitivity. The relative sensitivity of parameter ***x*** to the function ***f(x,y,z, …)*** is defined as follows:

$$\text{Relative Sensitivity} = x\frac{\partial f(x,y,z,\Lambda)}{\partial x}\bigg|_{x=x_1,y=y_1,z=z_1,\Lambda}$$

The classical (absolute) sensitivity can be used to evaluate the potential contribution of a

Parameter	Relative Sensitivity	Parameter	Relative Sensitivity	Parameter	Relative Sensitivity	Parameter	Relative Sensitivity
a_{w}	-0.729432	e_{w}	-0.157994	i_{w}	-0.205394	m_{w}	-100.046
a_{IJ}	-0.267943	e_{IJ}	-0.099276	i_{IJ}	-0.004087	m_{IJ}	-2.14555
b_{w}	-0.736727	f_{w}	-0.159574	i_{w}	-0.205394	o_{M}	-6.02563
b_{rr}	-27.0624	f_{rr}	-10.0269	i_{rr}	-0.004087	o_{r}	-6.16302
c_{w}	-0.119049	g_{w}	-0.452389	k_{w}	-0.998683	n_{rr}	-6.16302
c_{rr}	-0.119049	g_{rr}	-0.049618	k_{rr}	-0.020362	n_{w}	-6.02563
d_{w}	-0.120239	h_{w}	-0.456914	l_{w}	-0.998683	-	-
d_{rr}	-12.0239	h_{rr}	-5.01152	l_{rr}	-0.020362	-	-

Table 7 Relative Sensitivities for 30 Related Parameters for the Probability of Recovery Success

parameter to the output while varying same “amount” of each parameter. In contrast, the relative sensitivity can be used to evaluate the potential contribution of a parameter to the output while varying same “proportion” of each parameter. Therefore, if we assume that same amount of effort is required to decrease each parameter by a factor of 10, as an example, the relative sensitivity becomes the direct measure of the effort-effectiveness of each parameter. Table 7 shows relative sensitivities for 30 related parameters for the probability of recovery success, and encircled are the most sensitive parameters in this model.

According to the result of relative sensitivity analysis, it is found that the probability that human operators mistakenly take wrong actions is found to have the highest relative sensitivity in this model. This result comes from the fact that if the recovery actions of human operators become wrong, no matter how elaborately the recovery actions were prepared, the whole system will fail to recover from abnormal state. The design of complex systems such as the instrumentation system, the control/protection system, the display system, and the fault diagnosis system (in the high relative sensitivity order) is found to have high relative sensitivity. It seems that this is because the algorithms implemented in those systems have high probability of containing design faults, due to the complexity of the algorithms. The factors associated with human operators are also found to have high relative sensitivity in this model, as widely perceived.

Accident Analysis - the TMI-2 Accident

It is widely accepted that an accident is not the result of a single cause. Rather, it is the result of the mixture and combination of many complex causes. In other words, an accident is the result of a series failure to the recovery actions, which can be taken by the control/protection system or human operators. Because the model we are suggesting here is about evaluating the success and failure probabilities of the recovery actions, we believe that our model can be well applied for accident analysis, not only qualitatively, but also quantitatively.

The TMI-2 accident can be characterized as a loss-of-coolant-accident caused by stuck-open PORV(Pilot-Operated Relief Valve) and failure of human operators to recognize it. Based on the condition of the plant before the accident [3], the parameters in the model were assigned as in Table 7: According to the assumed parameter values for the TMI-2 nuclear power plant, the numerical result for the probability of recovery success is calculated. The numerical result is:

$P[failure] = 0.035728$ (※ $P[success] = 0.964272$)

Even though the failure probability is two orders higher than that of the example situation given above, the absolute value of the failure probability 0.036 (one failure of recovery in about 30 plant failures) does not seem to be that high. However, when considering the fact that the TMI-2 plant had such a poor history of equipments, a severe accident seems to have been inevitable.

It would be interesting to check the probability of recovery failure for the TMI-2 nuclear power plant when we assume that the human operators were well-trained or the reliabilities and the availabilities of the I&C systems and MMI were high to the degree of the example situation given above:

① Well-trained operators : P[failure]=0.019136 ($o_M=p_M=0.1$, $o_L=p_H=0.01$)

② High reliability I&C systems and MMI : P[failure]= 0.012426

($a_W=a_U=b_W=c_W=c_U=d_W=e_W=e_U=f_W=0.0001$, $b_U=d_U=f_U=0.01$)

①+ ② : P[failure]=0.001897

As shown above, if the operators of the plant were well trained, the probability of recovery failure decreased by a factor of 2. And, if the I&C system and MMI(even though there was only

the display system) were highly reliable, the probability of recovery failure decreased by a factor of 3. If these two conditions were satisfied together, the probability of recovery failure decreased by a factor of 20.

Therefore, we believe that we cannot blame the operators to be completely responsible for the accident, even though they were actively involved in the accident.

VI. Summary and Conclusions

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.

To identify key factors for the reliability of the system, the concept of 'relative sensitivity' is devised and relative sensitivity analysis is performed for the example. The relative sensitivity analysis shows that the probability of human operators mistakenly taking wrong actions is found to have the highest relative sensitivity in this model. The design of the instrumentation system, the control/protection system and other systems is found to have high relative sensitivities. The factors related tot human operators are also found to have high relative sensitivities. This model is applied to the analysis of the TMI-2 accident and reveals that the accident took place because of the combination of the failures in I&C system, MMI and human operators.

References

[1] Marc. Davio et al., "Discrete and Switching Functions", Georgi Publishing Company and McGraw-Hill International Book Company, 1978

[2] Catherine M. Thomson et al, "The Application of ATHEANA: A Technique for Human Error Analysis", *Proceedings of IEEE Sxth Annual Human Factors Meeting*, Orlando, Florida, 1997

[3] Nancy G. Leveson, "Safeware", Addison-Wesley Publishing Company, 1995