2009 International Nuclear Atlantic Conference - INAC 2009
Rio de Janeiro,RJ, Brazil, September27 to October 2, 2009
ASSOCIAÇÃO BRASILEIRA DE ENERGIA NUCLEAR - ABEN
ISBN: **978-85-99141-03-8**

A REVIEW OF THE MODELS FOR EVALUATING ORGANIZATIONAL FACTORS IN HUMAN RELIABILITY ANALYSIS

Marco Antonio Bayout Alvarenga[1], Paulo Fernando Ferreira Frutuoso e Melo[2], Renato Alves da Fonseca[1]

[1] Comissão Nacional de Energia Nuclear (CNEN)
Rua General Severiano, 90
22290-900 Rio de Janeiro, RJ
bayout@cnen.gov.br, rfonseca@cnen.gov.br

[2] COPPE/UFRJ – Programa de Engenharia Nuclear
Caixa Postal 68509, 21941-972 Rio de Janeiro, RJ
frutuoso@con.ufrj.br

ABSTRACT

Human factors should be evaluated in three hierarchical levels. The first level should concern the cognitive behavior of human beings during the control of processes that occur through the man-machine interface. Here, one evaluates human errors through human reliability models of first and second generation, like THERP, ASEP and HCR (first generation) and ATHEANA and CREAM (second generation). In the second level, the focus is in the cognitive behavior of human beings when they work in groups, as in nuclear power plants. The focus here is in the anthropological aspects that govern the interaction among human beings. In the third level, one is interested in the influence that the organizational culture exerts on human beings as well as on the tasks being performed. Here, one adds to the factors of the second level the economical and political aspects that shape the company organizational culture. Nowadays, the methodologies of HRA incorporate organizational factors in the group and organization levels through performance shaping factors. This work makes a critical evaluation of the deficiencies concerning human factors and evaluates the potential of quantitative techniques that have been proposed in the last decade to model organizational factors, including the interaction among groups, with the intention of eliminating this chronic deficiency of HRA models. Two important techniques will be discussed in this context: STAMP, based on system theory and FRAM, which aims at modeling the nonlinearities of socio-technical systems.

1. A CURRENT CRITIQUE ON NON-SYSTEMIC MODELS

USNRC published recently two NUREGs related to good practices in the field of Human Reliability Analysis (HRA). The first of these documents, NUREG-1792 [1] establishes the criteria of good practices the techniques and methodologies of HRA should comply with. The second document, NUREG-1842 [2], performs an evaluation of the main techniques or methodologies of HRA in comparison with the established criteria in NUREG-1792.

These documents recognize the fact that Performing Shaping Factors (PSFs) are important and help the HRA analysts identify and understand some influences that PSFs exert on the actions of the tasks allocated to human beings. They also recognize the fact that databases on plant operational events are useful to get data on the influences the operational context (including the organizational factors) exert upon the unsafe actions involving human failures and establish some quantitative base to quantify human errors probabilities (HEPs) as a function of organizational factors.

However, the above NUREGs do not emit any criteria or specific guides for the implementation of organizational factors in HRA, leaving this task as a suggestion for future research. In spite of recognizing certain efforts in this sense, as for example, Ref. [3], the NRC also admits that the state of the art in how to identify and to understand the important organizational influences and how to use this information for determining HEPs is not adequate until now.

The origin of the deficiency mentioned previously is in the model type that has been adopted so far for Probabilistic Safety Assessments (PSA) and Analysis of Operational Events (AOE), including several types of incidents and accidents. Let us start then to discuss the main characteristics of these models and how they can be altered to establish a correct paradigm, in order to treat organizational factors in an appropriate way.

In references [4-6], one can find the comparison between the traditional approach (non-systemic) and the systemic approach of risk assessment. Below we describe the main differences between them, pointed by those authors. There are three types of accident models and associated risk analyses: accident sequential models, accident epidemic models and accident systemic models.

The sequential models of accidents are those used in most of HRA and PSA techniques. These models are based on the hypothesis that accidents can evolve in a pre-defined sequence of events that involve failures of systems, components and human failures. It is part of the initial hypothesis that the global system that is being modeled can be decomposed in individual parts, in other words, systems, subsystems and components, described in the down-up direction (lower, physical hierarchical level to the higher, abstract hierarchical level).

Risks and failures are, therefore, analyzed in relation to events and individual components, with their associated probabilities. Human failures are treated just as component failures. The outputs (the effects in terms of catastrophic failures, e. g., core meltdown) of the global system are proportional to the inputs (causes in terms of individual failures), that are predictable for those that know the design of the subsystems and components); therefore, these systems are linear. The risks are represented by a linear combination of failures and malfunctioning, for example, observed in event trees and fault trees. Accidents are, therefore, avoided by the identification and elimination of the possible causes. The safety level can be assured by improving the answer of the organization that is responsible for the plant in reacting to the triggered accidents (robustness feature).

The hypotheses – decomposition, linearity and simple combinations of individual failures – work well strictly for technological systems, because system and component designers know how these systems and components can be decomposed in individual parts and how they work. Therefore, they can make reliable inferences on the modes of failure of such systems and components.

The epidemic models of accidents are equally based on the linearity and decomposition hypotheses, but they have complex characteristics, because they are based on more complex combinations of failures and mainly on safety barriers weaknesses. In this case, simple failures of systems and components, or human failures, combined with latent failures (design, maintenance, procedures, management, etc.) contribute to the degradation of safety barriers, thus affecting the defense in depth concept. The global system should be modeled from top to bottom, from the safety objectives and functions, hierarchically higher until the lower functional levels. Risks and failures can, therefore, be described in relation to the functional behavior of the whole system. Accidents are avoided by reinforcing safety barriers and thus the defense-in-depth concept. Safety is assured by monitoring these barriers and defenses, through safety action indicators.

On the other hand, socio-technical systems are by their very nature, complex, non-linear and non-decomposable. These three qualities appear naturally from a unique outstanding characteristic of these systems: they are emergent. The fact of being emergent means that the complex relationships among inputs (causes) and outputs (effects) make unexpected and disproportional consequences to emerge, which lead one to the resonance concept, in other words, certain combinations of the variability of system functional actions as a whole can achieve the threshold allowed for the variability of a system function. This is the approach of the systemic models of accidents.

The action variability is an immediate consequence of the nature of socio-technical systems that survive in social, economical and political environments. Those environments determine the variability index, because they are composed by human beings, with a highly adaptive cognitive and emotional character, with their own cognitive mechanisms, and they are not of a technical nature as found in common systems. Consequently, the functional variability behaves completely differently from that of systems composed by components only.

In this case, the risk analysis associated with these systems should leave aside the individual failures of systems and components to simulate the system dynamics as a whole, seeking for combinations of individual variability of the system functions that can lead to undesirable functional behaviors, after the propagation of these combinations through the whole system. This means that an individual part of the system is linked to the system as a whole. However, the risk analysis must pay attention to the dynamics of the whole system and not to the action or behavior of the individual part.

In this approach, accidents result from unexpected combinations (resonances) of the variability of action or behavior. Therefore, accidents can be avoided by monitoring and reducing variability. Safety is assured by the constant ability of anticipating future events.

Before detailing these systemic models of accidents, we will describe how the available HRA techniques, of first and second generation, treat organizational factors.

2. ORGANIZATIONAL FACTORS IN TECHNIQUE FOR HUMAN ERROR RATE PREDICTION (THERP) [7]

In the first generation methodologies of HRA, like THERP, organizational factors are taken into consideration by means of performance shaping factors (PSFs), which are multiplied by the basic human error probabilities (BHEPs), increasing or decreasing the baseline values. The NUREGs of good practices mentioned in the previous paragraph establish about fifteen PSFs that are important for HRA. These PSFs are described below:

1. quality of training/experience;

2. quality of procedures/administrative controls;
3. availability and clarity of instrumentation;
4. team available and time required to complete the act including the impact of concurrent activities;
5. complexity of the required diagnosis and response;
6. workload/time pressure/stress;
7. crew dynamics and characteristics (e.g., degree of independence among individuals, operator biases/rules, use of status checks, level of aggressiveness in implementing the procedures);
8. available staffing/resources;
9. ergonomic quality of the human-system interface;
10. environmental factors;
11. accessibility and operability of the equipment to be manipulated;
12. the need of special tools (e.g., keys, ladder, hoses, clothing);
13. communications (strategy and coordination) and whether one can be easily heard;
14. special fitness needs;
15. accident sequence diversions/deviations (e.g., extraneous alarms, outside discussions).

Among the 15 PSFs, only factors 1, 2 and 8 can be considered organizational factors. The others are cognitive characteristics (4, 5, 6, and 15), man-machine interface design features (3), design or ergonomics factors (9, 10, 11, 12, 13, and 14) or group interaction factors (7 and 13). The cognitive characteristics can be included in the error mechanisms of second generation HRA methods. The group factors can be interpreted as human factors of the second level (between human-machine interaction in the first level and organizational factors in the third level) and can be included in the organizational factors, related to management and supervision activities. Man-machine interface and ergonomics design characteristics are plant-specific features, but can be interpreted as the poor result of design processes having as root causes some deficient organizational factors. The design processes itself, however, is not modeled in THERP. In NUREG-1842 [2], there are several critiques about the use of PSFs in THERP. These critiques are reproduced below:

- PSFs are listed and discussed in Chapter 3 of THERP Handbook [7], which also presents their relevance; however, there is not a detailed orientation of how to quantitatively evaluate each PSF;
- THERP reveals explicit factors for stress levels and levels of experience only. For other qualitatively analyzed PSFs, it does not display explicit factors;
- Besides PSFs with explicit factors (stresses and experience), there are three additional groups of PSFs that may modify the nominal value of a HEP. However, that modification occurs in a subjective way:
  - PSFs already included in the nominal value of a HEP that are listed in THERP tables (for example: if the written procedure to be followed is long or short);
  - PSFs specified as rules that modify the nominal value of a HEP, inside its uncertainty limits (for example: to use the higher limit, if the operator involved in an action is not well trained).
  - PSFs for which there are not specific orientations with relation to the quantitative evaluation (factors).
- The quantitative evaluation of PSFs of the third group depends on the experts' experience and judgment in human factors or of human reliability analysts;

- The lack of orientation in the quantitative evaluation of PSFs can become a source of analyst’s or specialist’s variability when THERP is used. This feature can distort the results obtained in HRA and consequently in Probabilistic Safety Assessments (PSA);
- The quantitative evaluation of some PSFs can induce the analyst simply to assume that those are the most important PSFs, the ones that should be treated, in detriment of the remaining ones. Therefore, an inadequate quantification of HEPs can happen, because there can be other important PSFs not considered by the analyst.
- In the quantitative evaluation, it is also necessary to point out that THERP, due to its characteristics, does not treat organizational factors, so that possible latent PSFs that can influence HEPs are not treated in the analysis.

Besides the critiques described above, THERP linearly approaches the plant and consequently the organization in which it is inserted, therefore THERP does not consider the plant socio-technical characteristics that should be taken into account in the qualitative and quantitative analysis of PSFs.

3. ORGANIZATIONAL FACTORS IN SPAR-H [8]

SPAR-H evaluates the following eight PSFs: 1 available team; 2 stress; 3 complexity; 4 experience/training; 5 procedures; 6 ergonomics; 7 fitness for duty; and 8 work process. Among these, only 4, 5, 7, and 8 can be considered organizational factors. The others can be considered cognitive characteristics (1, 2, and 3) or ergonomics factors (6). SPAR-H suggests some metrics to calculate specific PSFs, like complexity, time pressure and available team. There are no specific suggestions, however, for the remaining ones, although it mentions research in this area through the technical literature The NUREGs of good practices [1-2] point out the following deficiencies of the SPAR-H methodology related to performance shaping factors:

- The approaches supplied by SPAR-H on how to evaluate the influences of a specific PSF are generally useful, but they can be insufficient to analyze and understand the conditions of a scenario. Those conditions affect the task of attributing levels (to generate factors) for each PSF, especially if analysts without enough knowledge of HRA and human factors are used in the measurement.
- The detailed analysis of PSFs presents inadequate solutions, because a nominal level (fixed factor) is almost always attributed to PSFs, due to the way they are defined, limiting its usefulness for identifying different situations. This approach has as an effect a generalization that assists some of the applications directed to SPAR-H, but it can be insufficient for detailed evaluations of plants or specific scenarios.
- In the analysis of complexity SPAR-H considers a multiplicity of factors (PSFs), guiding the analyst to a technical literature of orientation that makes it possible the evaluation of the factors. This approach does not seem appropriate for a method of simplified and normalized HRA, because it may go beyond the analyst's capacity that, for example, does not have enough knowledge on psychology. However, the discussion is healthy and can help the decision-making process in what concerns complexity.
- The orientation and the solution to measure the complexity are practical, useful and important, for a generic analysis. However, it can be inadequate for a detailed analysis of the plant or scenario.

- In the analysis of SPAR-H, the six training or experience months represent a parameter that is not applicable in many situations, because the plant operation team may have a member with less than six months of training or experience. The level, the frequency and the training type the team of a plant receives about the scenarios and actions related to the scenarios are much more important for the success of the action and these subjects are not approached in PSFs.
- The analysis of the generic PSFs named *fitness for duty*, seems not to be useful, as long as there is a nominal value for almost all cases in commercial nuclear plants. It is worth pointing out that PSFs are very important in the retrospective analysis of current events.

The good recommendation on SPAR-H methodology is the interaction between PSFs, including organizational factors, through the qualitative interaction matrix that is plant specific. SPAR-H does not suggest a quantification technique, but only the qualitative indication on how PSFs can be realistically and coherently quantified.

The approach of SPAR-H is to use the plant and specific scenario information to evaluate the effects of PSFs. However, in the calculation of HEPs, each PSF (eight) is treated independently from the remaining ones; in other words, the analysts will make judgments separately on each PSF. However, SPAR-H supplies a good discussion on the potential of the interaction effects among PSFs, due to the event and scenario specificities to be analyzed. Besides, it is certainly possible, and in many cases probable, that other factors (for example: team characteristics, procedure strategies) can influence the team action for a given scenario.

So, unless it happens an analysts' attempt (independently, without explicit orientation) to take into account such effects (in other words, to consider interactions), it is possible that the results do not reflect important plant and scenario specific characteristics. In other words, if the analysts do not try to incorporate the influences of the interaction potential effects among PSFs and do not include the influences of other important PSFs when necessary, taking into account the accident scenario, there is the possibility that the generic analysis does not supply a realistic evaluation of a specific accident or plant condition. Therefore, this is a limitation of SPAR-H.

If a generic high-level analysis is considered appropriate for a specific application (for example: the analysis of Accident Sequence Precursors [9]) or if after some analyses, the independent evaluation of all PSFs is considered appropriate for the event and for the scenario that will be examined, a simple application of SPAR-H can be appropriate. Otherwise, the results might contain errors and an important potential plant problem (for example, limitations in the procedures) might not be identified.

4. ORGANIZATIONAL FACTORS IN ATHEANA [10]

ATHEANA evaluates sixteen PSFs, shown in Table 1. The PSFs treated in ATHEANA should undergo an analysis with the purpose of covering subjects from plant design to plant organization. This classification aims just to break the linearity of classifying PSFs as mere multiplying factors - this approach needs to be enlarged. Table 1 sets a link between PSFs that can be considered as effects and their possible characteristics or generating factors.

Table 1. ATHEANA Performing Shaping Factors

Performing Shaping Factors	Characteristics and Factors
1. Quality of training/experience	**Organizational factors**: Possible failure in quality assurance. Important: within that factor is another factor, the latent factor, which hides the problem.
2. Quality of procedures/administrative controls	**Organizational factors:** Possible failure in quality assurance. Important: within that factor is another factor, the latent factor, which hides the problem.
3. Availability and clarity of instrumentation	Man-machine interface design features.
4. Time available and time required to complete the act including the impact of concurrent activities	Cognitive characteristics
5. Complexity of the required diagnosis and response	Cognitive characteristics
6. Workload/time pressure/stress	Cognitive characteristics
7. Crew dynamics and characteristics (e.g., degree of independence among individuals, operator biases/rules	Group interaction factors
8. Use of status checks, level of aggressiveness in implementing the procedures	Group interaction factors
9. Available staffing/resources	**Organizational factors:** Possible failure in quality assurance. Important: within that factor is another factor, the latent factor, which hides the problem.
10. Ergonomic quality of the human-system interface	Design ergonomics factors
11. Environmental factors	Design ergonomics factors
12. Accessibility and operability of the equipment to be manipulated	Design ergonomics factors
13. The need for special tools (e.g., keys, ladder, hoses, clothing)	Design ergonomics factors
14. Communications (strategy and coordination) and whether one can be easily heard	Design ergonomics factors or group interaction factors
15. Special fitness needs	Cognitive characteristics
16. Accident sequence diversions/deviations (e.g., extraneous alarms, outside discussions)	Special characteristics

It can be observed that the organizational factors described in Table 1 involve critical points like: training, procedures, administrative controls and human resources (personal). Considering training and procedures only, one is already in face of a binomial set of decisive factors in plant operation and safety. In spite of not being characterized as organizational factors, the other factors and described characteristics in Table 1 can be effects whose causes may be due to possible organizational fragilities.

For example, factors related to ergonomic designs can be the result of incorrect options taken during the design phase or even because of economical issues. Incorrect options and economical aspects are characterized as causes of organizational decisions. These observations have the sole intention of enlarging the understanding of human reliability experts.

The sixteen PSFs described in Table 1 are discussed in ATHEANA. A deeper study of PSFs is found in NUREG-1880 [11] which supplies additional information on expert judgment that allows for developing a PSF quantification process. NUREG-1624 [9] does not focus on this subject. Also, in Appendix B of NUREG-1792 [1] a discussion is presented on PSFs that it is consistent with ATHEANA's.

Unlike other HRA methods, which do not have a list of a priori defined PSFs, ATHEANA treats PSFs the same way other HRA methods do. These latter do not have a list of a priori defined PSFs in order to guide the users and, many times, multiplying factors are used to adjust HEPs. ATHEANA uses the context to identify PSFs and it evaluates the most important plant conditions that influence the human action being analyzed and can trigger PSFs. Therefore, although ATHEANA lists several important PSFs for most of the HEPs, experts can present other PSFs (positive or negative) that are judged to influence HEPs. Their estimation is performed by taking into account the plant conditions. So, instead of using a group of predetermined PSFs, they are obtained starting from the plant context evolution, analyzed by experts.

Experts in their judgment process to estimate HEPs use the context general information to obtain the best decision for each HEP. Due to the way PSFs are identified and considered in ATHEANA, it should simply be avoided the measure or evaluation of the influence degree of each PSF. The reason is because, as previously seen, ATHEANA uses the context evaluation to decide which PSFs are important or triggered by the context (former: the context is complex, because the procedure does not satisfactorily solve a specific situation) and, therefore, they are not pre-established multipliers for the influence degree of each PSF. As in many other HRA methods, the task to decide the way how PSFs affect the estimate of HEPs remains to experts.

Due to the importance of the appropriate context study, which includes important PSFs for the action that will be evaluated, it is important that experts that use ATHEANA identify the specific plant information and PSA scenarios to define the context and its influence on the human actions that are under analysis. Second generation techniques of HRA, like ATHEANA [10] and CREAM [12] use the cognitive model of the human being and the error mechanisms that influence human failures or unsafe actions. In these two approaches, there is the proposal of a prospective analysis that links PSFs with error mechanisms and error types or modes (unsafe actions). This analysis has qualitative features and there is, in the proposed quantification, the idea of taking into account the conditional probabilities given the pairs of PSFs (together with operational context) - error mechanisms and error mechanisms - unsafe actions (errors modes or error types) [13].

We must observe that in all the techniques above (first or second generation methods), the use of PSFs to describe factors that influence the basic human errors probabilities (BHEPs) are accomplished through a linear approach, because BHEPs are to be multiplied by these factors. Any organizational factors quantified in this way cannot take into account the nonlinearities of the socio-technical system.

5. FRAM (FUNCTIONAL RESONANCE ACCIDENT MODEL) [4]

In Section 1 we identified the concept of emergence as the main foundation of the systemic models of accidents. This concept was introduced by the English philosopher of science G. H. Lewes [14]. He proposed a distinction between resulting and emergent phenomena in which the resulting phenomena could be predictable starting from its constituent parts and the emergent phenomena could not.

According to the systemic models, failures emerge from the normal variability of the action of the functions that compose the system. The concept of functional variability carries us to the concept of functional resonance, which in turn can be derived from the stochastic resonance. This appears when a random noise is superposed to a weak signal in the output of the system or one of their component functions. The mixture of the two can reach or surpass the detection threshold of this signal, characterizing a stochastic resonance. Most of the time, in a stable condition, the variation or oscillation of the signal around a reference value remains within a variation range with very well defined boundaries, characterized by limit values. The variation of each signal depends on the interaction with other signals that exist in the system. For a specific signal, the other signals constitute the environment responsible for the noise, which represents the variability of this environment. Consequently, the functional resonance can be considered as the detectable signal that appears out of the non deliberate interaction of the weak variability of many signals interacting with each other.

Systemic models also have roots in chaos theory [15], which describes complex and dynamic systems. This kind of system can present unstable behavior as a function of a temporary variation of their parameters in a random way, even when the system is governed by physical laws. The consequence of this instability is that these systems can present a great sensitivity to disturbances (noise) and errors, which can be amplified by the system nonlinearities and the great number of interactions among the system components.

Chaos theory, however, has limited practical value to become a model of accidents according to Hollnagel [4], because the equations of the noise processes have to be added to the system equations. These, in turn, are formulated starting from physical laws describing the system. However, there are no deterministic equations and general physical laws for socio-technical systems. On the other hand, the management concept, a typically organizational factor, represents a control function. Several formulations have been proposed based on control systems [16] to model it. In 1997, Jens Rasmussen proposed a systemic model of the socio-technical system based on control systems [17].

Ref. [16] displays the basic model of control system theory for socio-technical systems. The model is composed of inputs, outputs, boundary conditions and feedback control. Another representation, the Structured Analysis and Design Technique (SADT) has been used for defining systems, analysis of software requirements and system and software design [18]. SADT consists of procedures that allow the analyst to decompose the software (or system) into several functions. An application example for modeling systems of nuclear power stations has been described by Rasmussen and Petersen [19]. The diagrammatic notation of SADT consists of blocks of functions, each one with three types of input parameters (inputs, controls and resources) and one of output (outputs). Hollnagel, in his FRAM model [4] extended this basic model by adding two more parameters: available time and pre-requirements.

In FRAM, the Functional Resonance Analysis is performed in four steps [4]:

1. Identify essential system functions through the six basic parameters mentioned above;
2. Characterize the potential variability (positive or negative) of each function as a function of the context;
3. Define functional resonance based on possible dependencies or couplings between these functions;
4. Identify barriers or damping factors to absorb the variability and specify required performance monitoring.

In the first step, the six basic parameters are described as follows [4]:

1. **Input**: what is used or transformed to produce the output;
2. **Output**: what is produced by a specific function;
3. **Control**: what supervises or adjusts the function;
4. **Resource**: what is needed or consumed by the function to process the inputs;
5. **Precondition**: system conditions that must be fulfilled before the function can be carried out;
6. **Time available**: it can be the constraint and can also be considered a special kind of resource.

In step 2 above, it becomes necessary to define the context to characterize the variability. There are two levels of context. The context of first order is defined internally by the complements of the systems functions. The context of second order is defined by the environment of the system. For a given function, the variability of the rest of the system defines its environment. The complement of the functions is supplied by the Common Performance Conditions (CPC). Each CPC affects one or more types or categories of functions, depending on the nature of the function. There are three categories of functions, in agreement with their nature: human (M), technological (T) and organizational (O).

Originally this was described by performance shaping factors, but in techniques like ATHEANA [10], evolved to the concept of error forcing conditions. In CREAM [12], PSFs appear under the name of Common Performance Conditions (CPC). All the CPC in CREAM influence all task steps as a whole. It is different from THERP, where specific PSFs influence specific task steps.

In CREAM, there are eleven CPCs and each one influences certain types of functions (M, O, or T):

1. availability of resources (M,T);
2. training and experience (M);
3. quality of communication (M,T);

4. human-machine interface (HMI) and operational support (T);
5. access to procedures and methods (M);
6. conditions of work (T,O);
7. number of goals and conflict resolution (M,O);
8. available time (time pressure) (M);
9. circadian rhythm (M);
10. crew collaboration quality (M);
11. quality and support of organization (O).

In order to quantify the effect of CPCs on function variability, a CPC gradation becomes necessary, although they are qualitative. Below we find Hollnagel's proposal on this gradation:

- Stable or variable but adequate - associated performance variability is low;
- Stable or variable but inadequate - associated performance variability is high;
- Unpredictable - associated performance variability is very high.

This proposal allows for quantification, if we associate values to the CPCs. The CPCs will influence all function parameters. If a parameter has the high performance variability value, the connections associated with this parameter will fail or be reduced. Consequently, we can see its impact on the whole network of functions, observing if the outputs of each function will fail or not.

In the third step of the analysis, the functional resonance is determined for the couplings between functions, established by the coupling among different function parameters. In other words, the output of a function can be connected to the different types of inputs of the other functions (input, resource, control and pre-condition). Through these couplings, one can identify how the variability of a given function can affect the action of the other functions. Either the function performance at the output or unexpected connections (functional resonance) between the functions can be discovered, thus invalidating (failing) the connection, or relaxing the coupling of the interconnected parameters in the connection. This is depicted in Figure 1.

In the fourth step of the analysis, safety barriers are identified to avoid the functional resonance. These barriers can be associated to any of the six function parameters, simply by adding one more connection (an AND logical node) to the pertinent parameter, which characterizes a restriction to the performance of that parameter in the function. However, there is another approach, which uses the same control system paradigm, but with a different kind of quantification, the STAMP model, which will be next described. The STAMP model uses a mathematical model to describe the system dynamics. It is different from FRAM, which uses the qualitative analysis (structural) based in connections and variability (semi-quantitative).

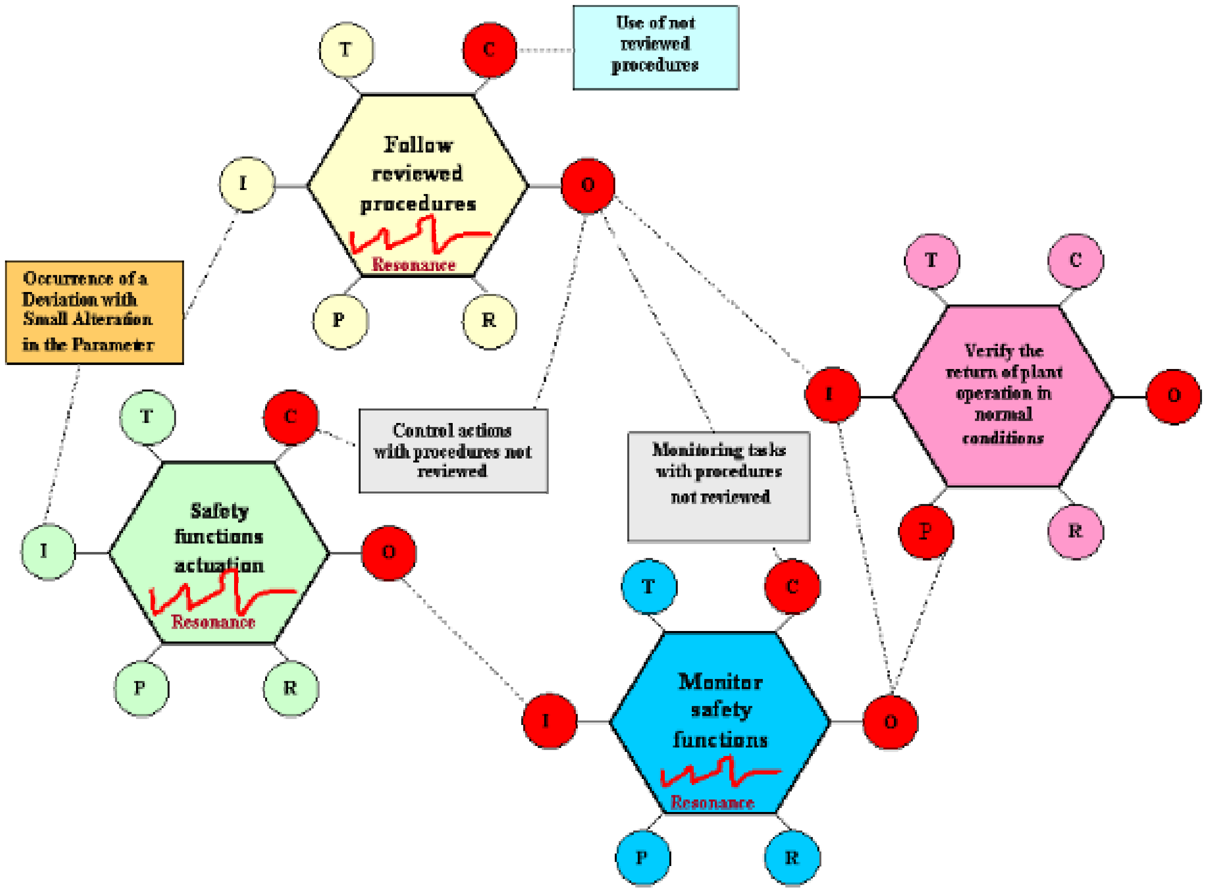
T
C
Use of not reviewed procedures
I
Follow reviewed procedures
Resonance
O
P
R
Occurrence of a Deviation with Small Alteration in the Parameter
T
C
I
Safety functions actuation
Resonance
O
P
R
Control actions with procedures not reviewed
Monitoring tasks with procedures not reviewed
T
C
I
Verify the return of plant operation in normal conditions
O
P
R
T
C
I
Monitor safety functions
Resonance
O
P
R

Figure 1. A functional resonance with safety function control and monitoring

6. STAMP (SYSTEMS-THEORETIC ACCIDENT MODEL AND PROCESS) [5]

STAMP is based on system process dynamics and not on events and human actions individually. Rasmussen [17] proposed a model for socio-technical-systems, where the accident is viewed as a complex process with several hierarchical control levels, involving legislators, regulators, elaborate associations, company policy, plant management, engineering/technical departments and operation staff (see Figure 2 and Refs. [20, 21].

Later, Rasmussen and Svedung [22] applied this model to risk management. However, they described the process downstream in each level through an event chain similar to event trees and fault trees. On the other hand, a model of socio-technical systems using the concepts of process control systems theory was applied by Forrester to business dynamics involving economic process [23]. STAMP combines the Rasmussen/Svedung structure with Forrester's mathematical model for system dynamics to describe the process occurring in each level.

The systemic model of STAMP leans on 4 basic concepts: Emergence, Hierarchy, Communication and Control. As discussed in the last section dedicated to the FRAM methodology, systemic models need the concept of emergence to explain the functional resonance. Accidents are seen as the result of the unexpected interaction (resonance) of system functions. Therefore, the components of these functions cannot be analyzed separately (individual failures) and later combined in a linear way to evaluate safety. Safety can only be evaluated by considering the relationship of each component with the other plant components, that is, in the global context. Therefore, the first fundamental concept of STAMP is that of underlying the emergent properties that are associated to the restrictions imposed on the degree of freedom of those components that compose the functions that belong to a given system hierarchy. The concept of system functions hierarchy becomes, therefore, the second fundamental concept [5, 24].

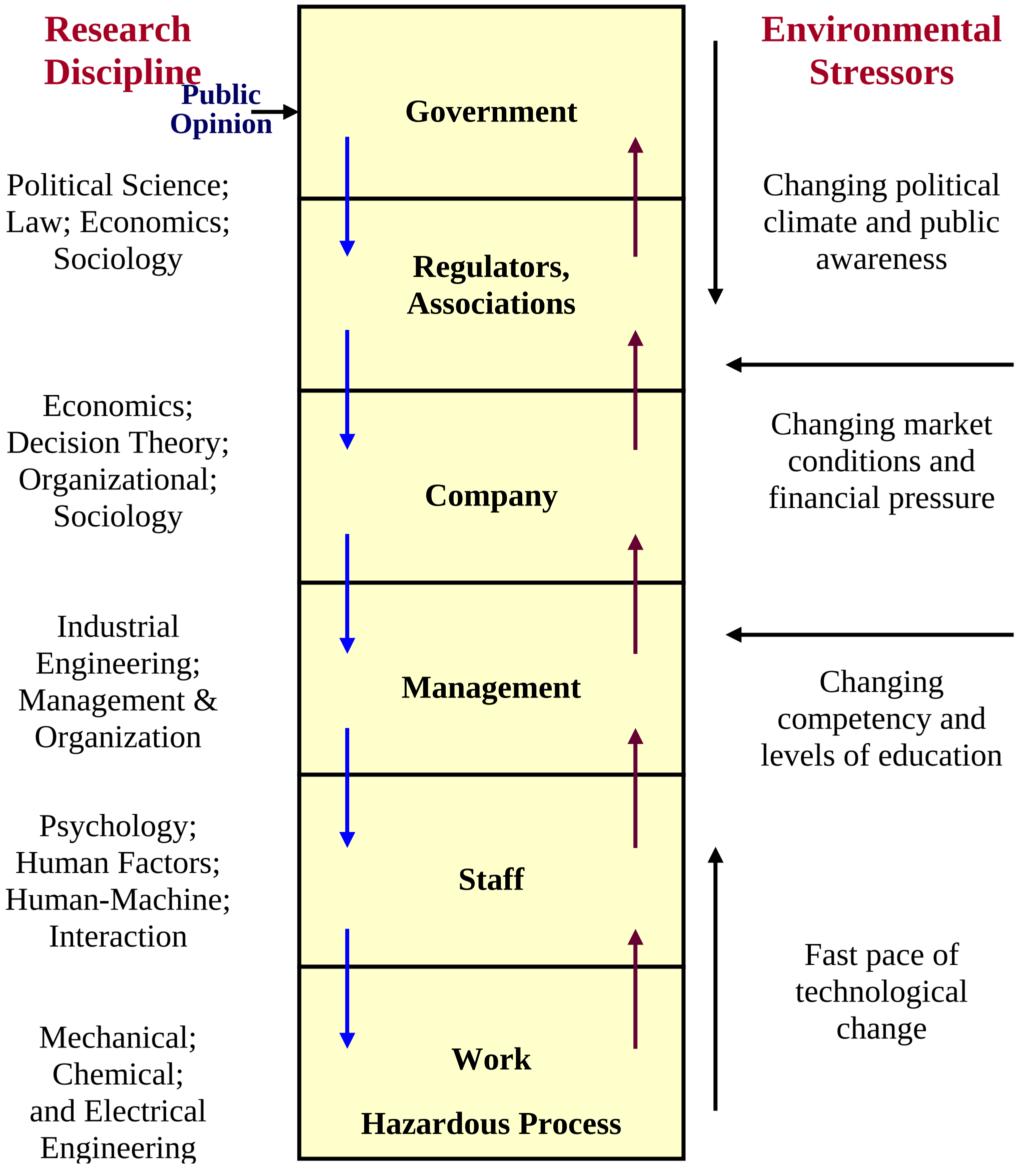
Research Discipline
Public Opinion
Government
Regulators, Associations
Company
Management
Staff
Work
Hazardous Process
Political Science; Law; Economics; Sociology
Economics; Decision Theory; Organizational; Sociology
Industrial Engineering; Management & Organization
Psychology; Human Factors; Human-Machine; Interaction
Mechanical; Chemical; and Electrical Engineering
Environmental Stressors
Changing political climate and public awareness
Changing market conditions and financial pressure
Changing competency and levels of education
Fast pace of technological change

Figure 2. The Socio-Technical Hierarchical System Involved in Risk Management ([21][20])

The emergent properties are controlled by a group of restrictions that represent the control actions about the behavior of the system components. Consequently, higher hierarchical levels impose restrictions or control actions on lower levels. Accidents appear, therefore, as the result of restriction violations for the interactions between components in the global context or because of the lack of appropriate control laws that are imposed in the execution of the restrictions [5, 24]. Due to the several hierarchical levels, the system is composed by several control loops nested through feedback mechanisms, other basic concept that comes from control theory (open systems that receive information from the environment to reach a steady state). These several feedbacks inside the system keep it permanently in a steady state, when constantly adapting to variations in itself and in the external environment. From this point of view, the accident is seen as the incapacity of the feedback in making the controls reinforce the restrictions execution. When the system components belong to the social and organizational levels, the restrictions take the form of internal policies, regulations, procedures, legislation, certifications, norms, authorizations, labor agreements and other instruments of economical, social, political and administrative control.

The other two fundamental concepts of STAMP are the controllers that exert the controls about the restrictions in the lower hierarchy levels and the effective channels of communication to transmit the control information and to receive the feedback information about the state of the restrictions. Comparing STAMP control structure with the parameters of the hexagonal structure of FRAM, we can identify two types of input parameters in FRAM, the Controls and the Pre-requirements are restrictions imposed on the behavior of the function to be controlled, while the Resources and the Available Time are part of the Inputs of the function. The output of the function is feedback for the controllers of higher hierarchical level.

Human or automatic controllers should exist in all hierarchy levels. Even in the automatic controllers' case, human beings will still be present in the monitoring of the automatic functions. Both types of controllers will need models to simulate the process that are controlled and the interfaces with the rest of the system to which they are interlinked. Some inputs to the controller are restrictions coming from the higher levels. On the other hand, the controller output supplies the restriction for the lower levels and the feedback of the state of the restrictions on its hierarchical level. These basic ideas are illustrated and detailed in [5, 24].

The controllers are not necessarily physical control devices, but they can be design principles, such as redundancies, interlocks and safe failure, or even processes, production and maintenance procedures. It is necessary to observe that human controllers possess a cognitive modeling [13]. Accidents happen when restrictions are not satisfied or controls on them are not effective. Therefore, in STAMP, the following accident causes are identified [5, 24]:

1. control actions exerting inadequate coercion related with restrictions
    a. unidentified hazards
    b. inadequate, inefficient or non existing control actions for the identified hazards
        i. Design of control algorithms of the processes that do not make coercion related with the restrictions:
            1. failures in the creation process
            2. changes of processes without corresponding changes in the control algorithm (asynchronous evolution)

3. incorrect modifications or adaptations

ii. inconsistent, incomplete or incorrect (alignment lack) processes models

1. failures in the creation process
2. failures in the updating process (asynchronous evolution)
3. time delays and inaccuracy measures that are not taken in consideration

iii. Inadequate coordination between controllers and decision makers (superimposing areas and boundaries)

c. inadequate execution of control action

i. failures of communication

ii. inadequate actuator operation

iii. time delays

d. inadequate or inexistent feedback

i. non provided arrangements in system design

ii. communication failures

iii. time delays

iv. Inadequate operation of sensors (incorrect information or not supplied).

The models should contain the same information either for human beings or automatic systems. The fundamental information is: relationships between system variables, current state of system variables, available process mechanisms for changing the state of system variables. The relationships between the system variables are modeled through the technique of system dynamics [5] that is based on the theory of non-linear dynamics and control through feedback. There are three basic blocks for building the models of system dynamics. These blocks perform basic feedback loops. The functions of each hierarchical level are composed of the complex coupling of several of these basic loops.

The first basic loop is the Reinforcement Loop, a structure that feeds itself, creating growth or decline, similarly to the loops of positive feedback in the theory of control systems. An increase in variable 1 implies an increase in variable 2, which causes an increase in variable 1, and so on, in an exponential way, if there are no external influences. The same reasoning is valid for a negative reinforcement, which generates an exponential decrease for one variable and an exponential increase for the other (reinforcements in the opposite directions), because an increase in a variable implies a decrease in the other variable. The change does not necessarily mean changes in the values but in the direction. In many instances, the variable is interacting with the variation rate of the other variable and not with the variable itself.

The second type of loop is the Balance Loop, in which the current value of a system variable or a reference parameter is modified through some control action. This corresponds to the loop of negative feedback in the theory of control systems. In this case, the difference between the variable value and the wanted or reference value is noted as an error. The action is proportional to the error, so that it brings the variable value to the reference value along time.

The third type is the Delay, which is used to model the time interval that elapses between the causes (or actions) and the effects. It could be the source of several instabilities in the system depending on the complex interactions between the system variables along time. Once the whole system is modeled through these basic structures, after the hierarchical functional decomposition and identification of the variables and parameters that define the functions, it becomes possible to accomplish the simulation of the system dynamic behavior, assuming certain initial values for the system variables. Consequently, the system can be observed along time to check for instabilities as well as abrupt behaviors, including the probable system collapse.

Marais and Leveson [25] discuss basic structures that can be identified in the dynamic simulation of systems that can erode or even cause the system collapse. These structures were named safety archetypes:

1. stagnant safety practices in face of technological progresses, due to delays in the control loops;
2. decreases in safety conscience due to the absence of incidents;
3. side effects due to unintended safety actions;
4. corrections of symptoms instead of root causes;
5. erosion of safety by:
    a. complacency - low rates of incidents and accidents encourage an anti-regulatory feeling;
    b. postponed safety programs - a conflict production versus safety;
    c. incident and event reports with lower priority - effects of the prize versus punishment strategy.

With the concept of safety archetypes associated to the STAMP methodology, it becomes a complete tool to model, simulate and evaluate the safety of socio-technical systems.

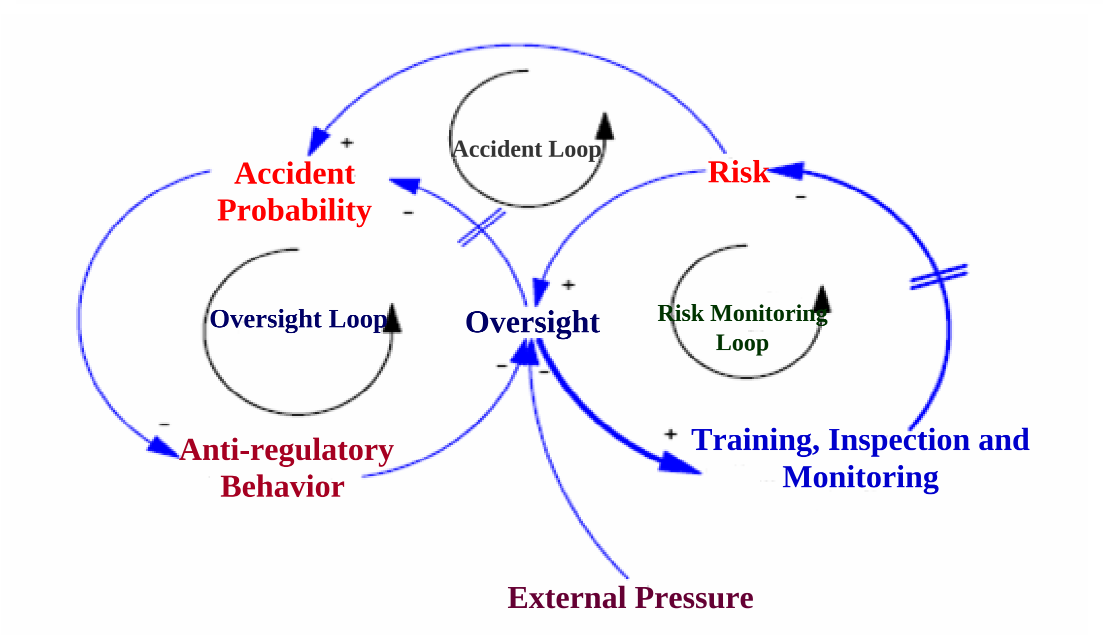

Figure 3. Example of a safety archetype (Complacency) [25]

7. CONCLUSIONS

The methodologies of human reliability analysis of first generation take organizational factors into consideration through performing shaping factors (PSFs). These factors are quantified in a subjective way by experts in the field of HRA or through databases of specific operational events for each plant that contains among the root causes the programmatic (or systematic) causes that characterize organizational factors. However, the interaction of these factors with error mechanisms and unsafe actions of human failures, or between the factors themselves is linear, because, according to the quantified level of the state of each factor, the probabilities of human error associated with unsafe actions are multiplied by adjusting factors that can decrease or increase them. The interconnection matrix between factors (see SPAR-H [8]) is also linear. HRA methodologies of the second generation continue to use PSFs, although they include in the network of conditional probabilities the error mechanisms as functions of the PSFs.

This approach has two basic deficiencies. The first is that the number of organizational factors is not enough to model all aspects of this nature, especially the political, economical and normative ones. On the other hand, the interaction of these factors with each other and with error mechanisms, unsafe actions, modes and types of errors observed in the individual level and group level is highly nonlinear.

Two modern approaches are the most promising to solve these deficiencies, because they are based on non-linear models: FRAM and STAMP. These two methodologies are based on the General Theory of Systems (GTS) [26] that largely uses the concepts of Control Systems Theory to accomplish in practice the basic ideas of GTS. The FRAM methodology extends the basic model of the theory of control systems with input and output variables or parameters, as well as for resources, controls or restrictions (boundary conditions), adding two more types of variables or parameters: time and pre-requirements that are considered special boundary conditions or special types of resources and restrictions. The socio-technical system is decomposed in functions and each function has a hexagonal structure as described in this paper. The system has internal feedback, because each hexagonal function is linked with the others through one or more of the six parameters or variable.

The nonlinear characteristic of FRAM is established by the resonance concept, in other words, given a limited variation in one of the parameters of one of the functions, the system can, in each information transmission for the interlinked functions, enhance the effect on other parameters of other functions and in its own function, which is generated in such a way so as to provoke an effect of stochastic resonance along time in the parameters that, in certain cycles of information transmission, can surpass its variation threshold, indicating a rupture in the system safety or stability. These transmission cycles for the functions can enter a process of stabilization or not, since the cycles can be dampened or not. Apart from the mathematical formulation for the stochastic resonance, Hollnagel establishes the concept of functional resonance, in which he tries to fail or relax the connections between the functions, through the six parameters or variables of interconnection. Thus, it is necessary to seek for unexpected connections between the functions. The failure or relaxation of the connection is a function of the parameters or variables variability in the connection. This variability, in turn, is a function of the variability of the Common Performance Conditions that influence all functions at the same time. Therefore, we can have several alterations in the parameters or variable values at the same time. This analysis is, therefore, of a qualitative or semi-quantitative nature, depending on the external subjective evaluations of CPCs. On the other hand, the concept of stochastic resonance can be worked through mathematical models as long as one establishes, in each function to be modeled, a mathematical function for the dependence of each one of the six variables or parameters as a function of the other five that compose the function. One should bear in mind, however, that the six components of the function can have one or more variables or representative parameters of the element, and this feature makes the modeling quite complex.

A proposal of establishing a mathematical model, as requested above, comes from the STAMP methodology that uses the modeling of system dynamics, used in economical systems. Although in this model a hexagonal structure is not used as in FRAM, it establishes in the same way a functional decomposition of the organization as a function of the organizational structure that is composed by several departments or divisions, each one with its specific function. They include the external organizations, such as the government, that interface with the organization. Each department has parameters and variables (P&Vs) in the input and output that make the interconnection with other departments or divisions. It also possesses P&Vs that represent the controls or restrictions of higher hierarchical levels, as well as P&Vs that represent resources to execute the function, including the time and pre-requirements as in the FRAM model. The dynamic simulation of these variables in STAMP is equivalent to the functional resonance in FRAM, with the advantage of identifying safety archetypes that are responsible for the system erosion and collapse, which serves as safety criteria to evaluate socio-technical systems.

REFERENCES

1. NUREG-1792, *Good Practices for Implementing Human Reliability Analysis*, U. S. Nuclear Regulatory Commission, Washington D.C., USA (2005).
2. NUREG-1842, *Evaluation of Human Reliability Analysis Methods Against Good Practices*, U. S. Nuclear Regulatory Commission, Washington D.C., USA (2006).
3. Davoudian, K., Wu, J. S. and Apostolakis, G. E., “Incorporating Organizational Factors into Risk Assessment through the Analysis of Work Processes”, *Reliability Engineering and System Safety*, **Vol. 45**, pp. 85–105 (1994).
4. Hollnagel, E., *Barriers and Accident Prevention*, Ashgate Publishing Company, Aldershot, United Kingdom (2004).
5. Leveson, N. G., *System Safety Engineering: Back to the Future*, Massachusetts Institute of Technology, http://sunnyday.mit.edu/book2.pdf, Cambridge, USA (2002).
6. Reason, J., *Managing the Risks of Organizational Accidents*, Ashgate Publishing Company, Aldershot, United Kingdom (1997).
7. Swain, A.D., and H.E. Guttmann, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, DC, USA (1983).
8. Gertman, D.I., H.S. Blackman, J. Byers, L. Haney, C. Smith, and J. Marble, *The SPAR-H Method*, NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Washington, DC, USA (2005).
9. NUREG/CR-4674, *Precursors to Potential Severe Core Damage Accidents: 1992, A Status Report*, Oak Ridge National Laboratory, U. S. Nuclear Regulatory Commission, Washington, D. C., USA (1992).
10. NUREG-1624, *Technical Basis and Implementation Guidelines for A Technique for*

Human Event Analysis (ATHEANA), U.S. Nuclear Regulatory Commission, Washington, D. C., USA (2000).

11. Forester, J., Kolaczkowski, A., Cooper, S., Bley, D., and Lois, E., *ATHEANA User's Guide Final Report*, NUREG-1880**,** U. S. Nuclear Regulatory Commission, Washington,D.C., USA (2007).
12. Hollnagel, E., *Cognitive Reliability and Error Analysis Method (CREAM).* Elsevier Science, New York (1998).
13. Alvarenga, M.A.B and Fonseca, R. A. "Comparison of the THERP quantitative tables with the human reliability analysis techniques of second generation", to be presented at ENFIR (2009).
14. Lewes, G. H., *Problems of life and mind. First Series: The foundations of a creed,* **Vol. 2**, University of Michigan Library Reprinting Series, Ann Arbor, USA (2005).
15. Lorentz, E., *The Essence of Chaos*, Rutledge, London, United Kingdom (2003).
16. Rasmussen, J., Pejtersen, A.M., and Goodstein, L.P., *Cognitive System Engineering*, John Wiley & Sons, New York, USA (1994).
17. Rasmussen, J., "Risk Management in a Dynamic Society: A Modeling Problem", *Safety Science*, **Vol. 27**, pp.183–213 (1997).
18. Pressman, R.S., *Software Engineering – A Practitioner's Approach*, McGraw-Hill Book Company, New York, USA (1992).
19. Rasmussen, B. and Petersen, K. E., "Plant Functional Modeling as a Basis for Assessing the Impact of Management on Plant Safety", *Reliability Engineering and System Safety*, **Vol. 64**, pp. 201-207 (1999).
20. Qureshi, Z. H., "A Review of Accident Modelling Approaches for Complex Socio-Technical Systems", Proceedings of the 12th Australian Workshop on Safety Related Programmable Systems, pp. 47-59, Australian Computer Society, Adelaide, Australia (2007).
21. Rasmussen, J., "Risk Management in a Dynamic Society: A Modelling Problem", *Safety Science*, **Vol. 27**, pp. 183-213 (1997).
22. Rasmussen, J., and Svedung, I., *Proactive Risk Management in a Dynamic Society*, Swedish Rescue Services Agency, Stockholm, Sweden (2000).
23. Forrester, J.W., *Industrial Dynamics*, MIT Press, Cambridge, USA (1961).
24. Leveson, N. G., "A New Accident Model for Engineering Safer Systems", *Safety Science*, **Vol. 42,** No. 4, pg. 237-270 (2004).
25. Marais, K. and Leveson, N. G., "Archetypes for Organizational Safety", *Safety Science*, **Vol. 44,** pp. 565-582 (2006).
26. Bertalanffy, L., v., *General Systems Theory, Foundations, Development, Applications*, Allen Lane, The Penguin Press, London, United Kingdom, 1971.