HUMAN RELIABILITY ANALYSIS OF THREE MILE ISLAND II ACCIDENT CONSIDERING THERP AND ATHEANA METHODOLOGIES

Renato Alves Fonseca, rfonseca@cnen.gov.br
Brazilian Nuclear Energy Commission – CNEN. Rua General Severiano 90, CEP: 22290-901, Rio de Janeiro, Brazil

Antonio Carlos Marques Alvim, Alvim@con.ufrj.br
Federal University of Rio de Janeiro – UFRJ. Av. Horácio Macedo, Bloco G, 206, CEP: 21941-914, Rio de Janeiro, Brazil

Paulo Fernando Ferreira Frutuoso e Melo**,** frutuoso@con.ufrj.br
Federal University of Rio de Janeiro – UFRJ. Av. Horácio Macedo, Bloco G, 206, CEP: 21941-914, Rio de Janeiro, Brazil

Marco Antonio Bayout Alvarenga, bayout@cnen.gov.br
Brazilian Nuclear Energy Commission – CNEN. Rua General Severiano 90, CEP: 22290-901, Rio de Janeiro, Brazil

Sonia Maria Orlando Gibelli, sonia@cnen.gov.br
Brazilian Nuclear Energy Commission – CNEN. Rua General Severiano 90, CEP: 22290-901, Rio de Janeiro, Brazil

Abstract. *The main purpose of this work is to perform a human reliability analysis using THERP (Technique for Human Error Prediction) and ATHEANA (A Technique for Human Error Analysis) methodologies, as well as their application to the development of qualitative and quantitative analysis of a nuclear power plant accident. The accident selected was the one that occurred at the Three Mile Island (TMI) Unit 2 Pressurized Water Reactor (PWR) nuclear power plan. The accident analysis has revealed a series of unsafe actions that resulted in permanent loss of the unit. This study also aims at enhancing the understanding of THERP and ATHEANA methodologies and their possible interactions with practical applications. The TMI accident analysis has pointed out the possibility of integration of THERP and ATHEANA methodologies. In this work, the integration between both methodologies is developed in a way to allow better understanding of the influence of operational context on human errors.*

Keywords*: Human Reliability Analysis; Plant Conditions; Error Mechanisms; Pre-Accidental Factors*

1. Introduction

The goal of reliability studies of component, equipment and systems is to detect potential failures. These studies envision minimizing risks through the use of reliability analysis, which is based on a Probabilistic Safety Assessment (PSA) study. The use of PSA as a tool allows the investigation of system failure probabilities, as well as helps to improve design issues from system development to its obsolescence.

Although reliability analysis is a breakthrough, it does not take into account errors that can be committed by operators or maintenance staff during plant operation. Such errors can cause either a plant transient or a shutdown, which has led experts to develop studies on Human Error Probability (HEP) considering the limitations akin to human behavior complexity.

In view of this, Human Reliability Analysis (HRA) studies were developed and improved, aiming at human error (HE) analysis, its origins and consequences.

In the well known WASH 1400 report, HRA received formal treatment (NUREG-75/014, 1975). The experts in the nuclear area are the precursors of the HRA studies. The first steps taken by these experts were to include psychological and physiological stressors, organismic factors, situational, task and equipment characteristics, into the HRA studies. This vision has been intensified in the ATHEANA methodology (NUREG/CR-6350, 1996 and NUREG-1624, 2000), which encompasses operational staff behavior, concerning operational contexts, error mechanisms, plant conditions and deviations from the nominal scenario. The analysis of these aspects is important to enhance system performance.

In this work, the accident selected for analysis was the one that occurred at TMI, which resulted in the decommissioning of Unit 2. As this important accident constitutes a mark in the nuclear energy generation history, lessons learned from it could also be applied to other industrial areas.

This study develops an innovative analysis on the possibility of integrating the pre-accidental and the post-accidental contexts of TMI accident, which can make the accident analysis more comprehensive and realistic.

In the pre-accidental context, a qualitative analysis is performed, by means of the use of ATHEANA (NUREG/CR-6350, 1996 and NUREG-1624, 2000), which considers the essential factors for TMI plant modeling. On the other hand,

THERP methodology (NUREG/CR-1278, 1983) is quantitatively applied to the post-accidental context, through its HEP tables. In should be emphasized that the results of the pre-accidental context are incorporated to the post-accidental ones.

2. Safety Probabilistic Evaluation Model

The ATHEANA methodology (NUREG/CR-6350, 1996 and NUREG-1624, 2000) states a variety of paths to be used to perform a probabilistic safety analysis (PSA) aiming at building a structure of logical models. The traditional logical models used are (1) the inductive logical model – Event Trees and (2) the deductive logical mode – Fault Trees. Such models are built to identify plant scenarios including human error events. These models are also used to identify the relation between temporal and causal aspects, although during the accident sequence course, they do not precisely define the events related to human behavior (NUREG/CR-6350, 1996 and NUREG-1624, 2000).

In addition to that limitation, other issues should be considered when it comes to logical models (NUREG/CR-6350, 1996 and NUREG-1624, 2000):

- The human failure events do not clearly define the possible influences into the operator performance;
- Instrumentation failures that can cause impact on operator response are not well specified;
- Some of the plant conditions are not adequately characterized with respect to their influences on operator performance;
- Some issues that can influence the error-forcing context, which can lead to an operator error, are not taken into account.

However, ATHEANA methodology (NUREG/CR-6350, 1996 and NUREG-1624, 2000) deals with the above mentioned limitations and clearly addresses the accident modeling, considering the plant pre-accidental context. It is important to notice that this analysis enables a better understanding on the applicability of the tables of the THERP methodology (NUREG/CR-1278, 1983). In this work, the ATHEANA methodology (NUREG/CR-6350, 1996 and NUREG-1624, 2000) is integrated to THERP (NUREG/CR-1278, 1983), which allows to quantify the likelihood of human error. This integration establishes an intermediate methodology which is the outcome of an innovative vision within the human reliability concept.

3. Topics of the Probabilistic Safety Analysis and Human Reliability Analysis Modeling

3.1 Plant Conditions

It represents the factors (operational and organizational) that can influence the plant operator performance (NUREG/CR-6350, 1996 and NUREG-1624, 2000). It characterizes the circumstances in which operator activities are affected by the performance shaping factors (NUREG-1624, 2000). These factors include: plant configuration aspects, process parameters and off-nominal conditions (NUREG/CR-6350, 1996 and NUREG-1624, 2000).

3.2 Performance Shaping Factors

These factors represent the context influences that may affect the human behavior. Due to that, an event of human failure can occur (NUREG-1624, 2000). The performance shaping factors are defined in NUREG/CR-5455, 1993 and NUREG/CR-1278, 1983.

3.3 Error – Forcing Context

This context represents the combination of performance shaping factors effects and plant conditions that together create a favorable situation to human error occurrence (NUREG/CR-6350, 1996 and NUREG-1624, 2000).

3.4 Error Mechanisms

Error mechanisms represent the characteristics of the cognitive process of information that influence the performance of operators and plant personnel, which can result in unsafe actions (NUREG/CR-6350, 1996 and NUREG-1624, 2000). The error mechanisms can appear during the following situations: Detection, Evaluation, Response Planning and Response Implementation (NUREG/CR-6350, 1996 and NUREG-1624, 2000).

3.5 Unsafe Action

Unsafe actions represent actions inappropriately taken by the plant personnel, or actions not taken when necessary, which result in the degradation of the plant safety condition (NUREG/CR-6350, 1996 and NUREG-1624, 2000).

3.6 Human Error

Human errors are characterized as the divergences between actions actually taken and the ones that should have been taken (NUREG/CR-6350, 1996 and NUREG-1624, 2000).

3.7 Human Error Event

Human failure events are modeled in the HRA to represent the failure of a function, system, and/or component as a result of an unsafe action, which results in a worsened plant condition (NUREG/CR-6350, 1996 and NUREG-1624, 2000). The HE event can be classified as commission error (improper application of a procedure) or an omission error (omission of a procedure that should be executed) (NUREG/CR-6350, 1996 and NUREG-1624, 2000).

3.8 Scenario Definition

Plant scenario comprises of minimum descriptions of the plant context required to develop the PSA Model, defining the appropriate human failure events (NUREG/CR-6350, 1996 and NUREG-1624, 2000).

4. Dependence

Dependence is defined as occurring among people. Dependence can also happen among different tasks performed by the same person (NUREG/CR-1278, 1983).

4.1. Defining the Levels of Dependence

- Zero Dependence: the error or success in performing a task does not imply in error or success of the subsequent task
- Low Dependence: there is a smallest influence between the performances of a task and the subsequent task
- Moderate Dependence: there is an obvious influence between the performances of a task and the subsequent task
- High Dependence: the performance of a task substantially affects the performance of the subsequent task
- Complete Dependence: the error or success in performing a task implies error or success of the subsequent task

4.2 Dependence Equations

Table 1 – Dependence Equations

Levels of Dependence	Equations
CD - Complete Dependence	B = 1
HD - High Dependence	B = [1 + HEP] / 2
MD - Moderate Dependence	B = [1 + (6HEP)] / 7
LD - Low Dependence	B = [1 + (19HEP)] / 20
ZD - Zero Dependence	B = HEP
B represents the probability of human error in the task based on the dependence level, and the abbreviator HEP represents the probability of human error on a task (NUREG/CR-1278, 1983).	

5. Pre-Accidental Analysis of the Three Mile Island Accident

The pre-accidental analysis points out that plant context can gradually lead the operational staff, within an error-forcing context, to take unsafe actions. It is also necessary to consider the performance shaping factors related to the pre-accidental context. These factors may turn an incident into an accident.

In the pre-accidental context is necessary to analyze the plant, checking its degree of availability and reliability. It should be also checked the type of maintenance, plant technology, interpersonal relationships, organizational ethics, etc. In this work, the pre-accidental analysis is based on NUREG-0600 statements.

5.1 System Failures in the Pre–Accidental Context

In the pre-accidental context, failures were found in the Primary System, specifically in the Reactor Cooling System, as well as in the Secondary System, explicitly in the Condensate System, Compressed Air System and Electrical System (NUREG-0600, 1979).

.

5.2 Pre-Accidental Context

In the pre-accidental context, the qualitative aspects of ATHEANA methodology (NUREG/CR-6350, 1996 and NUREG-1624, 2000) are integrated to THERP (NUREG/CR-1278, 1983). Based on that, the tables that show HEP, presented on THERP, can deal with the pre-accidental context. This analysis demonstrates that THERP can still be considered a useful tool.

5.2.1 Plant Conditions

- Plant Configuration: Plant configuration has indicated the existence of operational problems in the Reactor Cooling System, Condensate System, Feedwater System, Compressed Air System and Electrical System (NUREG-0600, 1979).
- Process Parameters: Plant parameters such as temperature, pressure and coolant inventory related to the Reactor Cooling System were not in compliance with the standards (NUREG-0600, 1979).
- Off-nominal conditions: Plant conditions related to the leak through the pressurizer safety valve together with the above mentioned process parameters were not in compliance with safety principles (NUREG-0600, 1979).

5.2.2 Performance Shaping Factor

- Organizational Factors: The existence of a leak in the reactor cooling system through the pressurizer relief valve was already known by the plant staff, as well as the design limitation of the condenser and the water intake into the instrument air system. These facts indicate the previous existence of plant organizational failures (NUREG-0600, 1979).
- Job Instructions: The pre-accidental context had shown a situation where procedures and standards were not met. Moreover, the working conditions were inadequate or plant staff was not sufficiently trained to comprehend the plant context. It should be emphasized that NUREG-0600 states that plant staff had already, at the time, enough operational experience.
- Tasks Characteristics: The critical tasks need to be correctly interpreted by the control room personnel, who should have a deep knowledge of the plant. They should also be able to anticipate events and establish a safe action based on the plant context (NUREG-1624, 2000). In TMI accident, human performance in the pre-accidental and post-accidental contexts contributed to worsen the course of the accident.
- Stress: Plant staff used to deal with plant non compliances, which possibly created an extra workload leading to stressing situations (Servan-Schreiber, 2004).

5.2.3 Error-Forcing Context

The TMI accident analysis has shown that error-forcing contexts arisen from the combination of performance shaping factors with plant conditions have created an environment in which HE occurrence was only a matter of time.

5.2.4 Error Mechanisms

The error mechanism that most influenced the pre-accidental context was the previous incorrect assessment phase (application of incorrect rules, misapplication of correct rules). Moreover, another error mechanism of detection phase has also occurred (attention failure or memory failure induced by man-machine problems and maintenance supervision failure). Both error mechanisms are linked to factors such as: workload, stress and inadequate human-machine interface (NUREG/CR-6350, 1996).

5.2.5 Unsafe Actions

In the pre-accidental context, unsafe actions are related to inappropriate actions such as, (1) emergency feedwater block valves left shut, (2) use of instrument air to try to release blocked resin in the transfer line and (3) high pressure injection throttling to prevent the pressurizer to became solid. Moreover, training provided to the staff was inadequate (NUREG/CR-6350, 1996 and NUREG-0600, 1979).

5.2.6 Off-Nominal Condition (Deviation from the expected scenario)

The failures that occurred in the plant (emergency feedwater block valves were closed and pressurizer relief valve did not closed after opening), have also induced the plant staff to commit HE (NUREG/CR-6350, 1996 and NUREG-0600, 1979).

5.3 Analysis of the Pre-Accidental Factors

The pre-accidental factors are originated from the integration of THERP (NUREG/CR-1278, 1983) and ATHEANA (NUREG/CR-6350, 1996 and NUREG-1624, 2000) methodologies. This analysis mostly comprises verification of the plant characteristics, as well as the performance shaping factors that have occurred prior to the event, which can influence the course of an incident or an accident. Each plant context is subdivided into a few items (characteristics) to be taken into account in order to allow the quantification of factors, which will be used to correct the HEP associated with the context.

5.3.1 Characteristics

- Design Characteristics
- Maintenance Characteristics
- Technological Updating Characteristics
- Ergonomic Characteristics
- Equipment Technical Specification
- Human Resource Management

5.4 Classification of the Operational Quality Levels and Pre-Accidental Factors

Table 2 – Operational levels based on pre-accidental factors

Operational Level 1	
Plant is operating under adequate operational and safety standards.	
Pre-Accidental Factor = 1 (Skilled Operator)	**Pre-Accidental Factor = 1 (Novice)**
Operational Level 2	
Plant requires few operational reviews without which, safety will be jeopardized in the long run.	
Pre-Accidental Factor = 1 (Skilled Operator)	**Pre-Accidental Factor = 2 (Novice)**
Operational Level 3	
Plant requires operational reviews without which safety will be jeopardized in the medium run.	
Pre-Accidental Factor = 2 (Skilled Operators)	**Pre-Accidental Factor = 4 (Novice)**
Operational Level 4	
Plant requires shutdown to allow operational safety review.	
Pre-Accidental Factor = 5 (Skilled Operators)	**Pre-Accidental Factor = 10 (Novice)**
Operational Level 5	
Plant requires partial design basis backfitting. Safety is jeopardized.	
HEP = 0.25 (Skilled Operator)	**HEP = 0.50 (Novice)**
Operational Level 6	
Plant requires total design backfitting. Safety is greatly jeopardized.	
HEP = 0.50 (Skilled Operator)	**HEP = 1.00 (Novice)**
Operational Level 7	
Plant must be shutdown	
HEP = 1.00 (Skilled Operator or Novice)	

In the TMI accident, the pre-accidental factor is of Operational Level 4: Plant requires shutdown to allow operational safety review. For example, in Operational Level 4, any HEP in the pre-accidental or post-accidental contexts, should be multiplied by a factor of 5 for skilled operator or by a factor of 10 for novice operator. The goal of this proposal is to include the influence of the plant operational context into the human error probability, within the pre-accidental context.

5.5 Event Tree of the Pre-Accidental Context

There was a HE in the TMI pre-accidental context: due to negligence, EF-V-12A and EF-V-12B valves had been left closed after the emergency feedwater valve test (NUREG-0600, 1979). Should the emergency feedwater system be required under operational incident conditions, it would have been unavailable, unless the valves were manually opened (NUREG-0600, 1979). The calculation of the HEP in leaving valves closed can be done as follows:

5.5.1 Operational Level 1- Plant is operating under adequate operational and safety standards

Task A comprises the emergency feedwater valve test. The HEP of this task, which is 1.0E-02, is described on Table 20-6 (NUREG/CR-1278, 1983). The HE of Task A lies on the fact that the crew forgot to open the feedwater valves after the test.

Task B comprises the verification of valves original positions after the test. The HEP of this task, which is 1.0E-01, is described on Table 20-22 (NUREG/CR-1278, 1983). The HE of Task B is the lack of verification whether the valves have been left closed.

5.5.1.1 Dependence Levels

To calculate the HEP it should be taken into account the level of dependence between test and inspection teams. In order to include that dependence, a few parameters need necessarily be considered:

- Take into account, as a conservative attitude, a low level of dependence between the teams (test and inspection) in the Task B.
- Take into account, as a conservative attitude, a high level of dependence between the acts of closing both valves. In case a valve has been left closed, it is very likely that the other valve is also left in the same position.

The HEP associated with the fact that valve EF-V-12A has been left closed, in tasks A and B, and the low dependence between teams are shown in Figure 1.

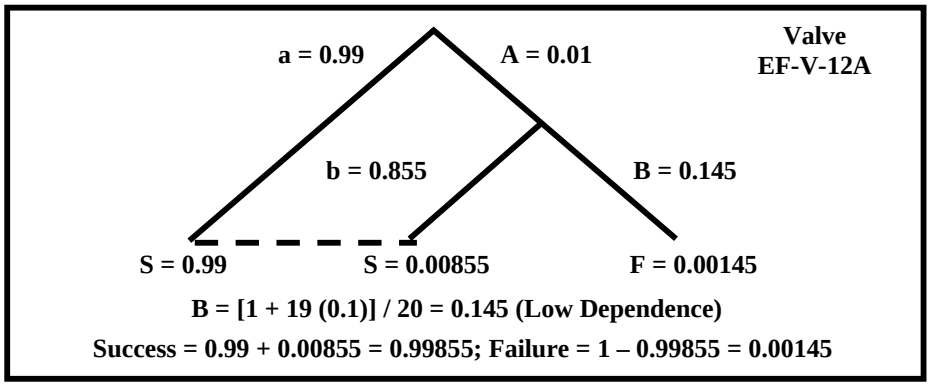

Figure 1 – Event Tree - Low dependency between teams in Task B

Capital letters represent error likelihood, whereas small letters stand for success. The HEP of EF-V-12A valve left closed is 1.45E-03, showed on Figure 1, which is the same probability value for leaving EF-V-12B closed, considering a level of independence between them.

Both EF-V-12B and EF-V-12A valves have been left closed due to high dependency between teams, which is shown in Figure 2. Figure 2 shows, in the first level, the error probability A and success probability a, both related to valve EF-V-12A. In the second level, the error probability B and success probability b are both related to valve EF-V-12B, which value is modified due to high dependency level between teams. The error probability of valves EF-V-12B and EF-V-12A is 7.3E-04, as can be seen in Figure 2.

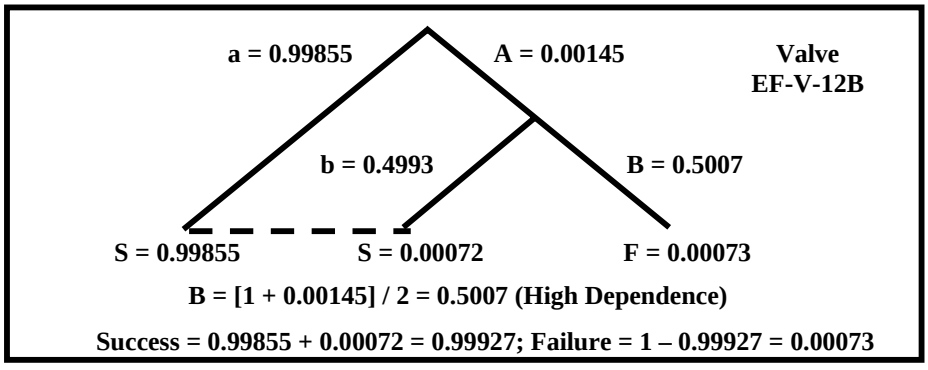

Figure 2 – Event Tree. High dependence between teams that operates EF-V-12A and EF-V-12B valves

5.5.1.2 Error Factors

The task involves the above mentioned test with associated error probability of 7.3E-04, which is less than 1.0E-03. Therefore, the associated error factor is 10, as can be seen on item 1, Table 20-20 (NUREG/CR-1278, 1983). Thus, it is possible to calculate the uncertainty limits: Lower Bound =7.3E-05; Upper Bound =7.3E-03.

5.5.2 Operational Level 4 - Plant requires shutdown to allow operational safety review

The TMI pre-accidental scenario is of Operational Level 4, as shown in Table 2. This means that any HEP, either in the pre-accidental or in the post-accidental contexts can be obtained by means of the multiplication of a Factor 5, in the case of a skilled operator, and a Factor of 10 for a novice one.

The Task A, that has a HEP of 1.0E-02, reaches a probability of 5.0E-02 while Task B, that has a HEP of 1.0E-01, reaches a probability of 5.0E-01. Figures 3 and 4 show the event trees and the HEP related calculations, considering the dependences.

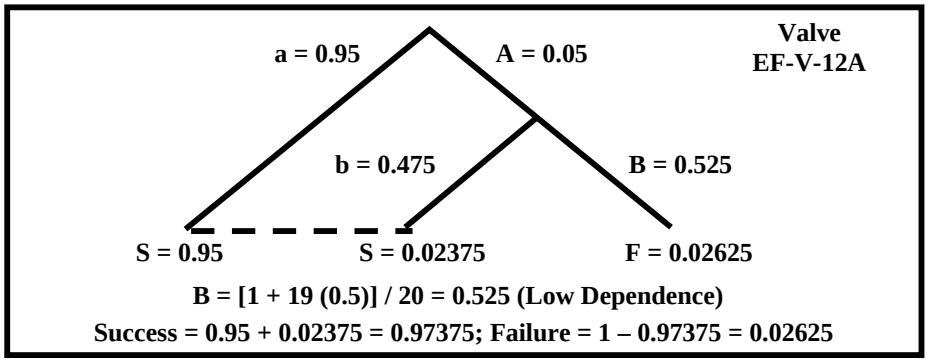

Figure 3 – Event Trees. Low dependency between teams in Task B

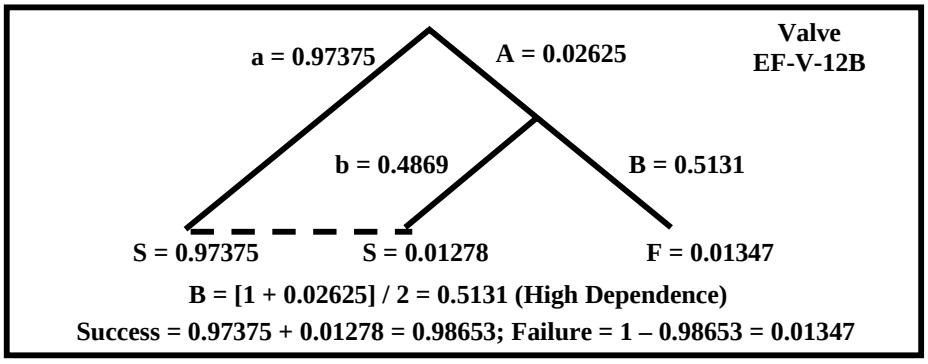

Figure 4 – Event Trees. High dependence between teams that operates EF-V-12A and EF-V-12B valves

5.5.2.1 Error Factors

The task involves the above mentioned system test with associated error probability of 1.347E-02, which is greater than 1.0E-02. Therefore, the associated error factor is 5, which can be seen on item 3, Table 20-20 (NUREG/CR-1278, 1983). Thus, it is possible to calculate the uncertainty limits: Lower Bound =2.7E-03; Upper Bound = 6.8E-02.

It is worthwhile to compare the results obtained for Levels 1 and 4. The HEP results obtained for Level 1 are related to nominal values from THERP table (NUREG/CR-1278, 1983); On the other hand, the HEP results obtained for Level 4 have the HEP values multiplied by a Pre-Accidental Factor 5. The upper bound limit is adopted for both Levels 1 and 4 due to the adopted conservative attitude.

- Results obtained for Level 1: 7.3E-03 or 0.73%
- Results obtained for Level 4: 6.8E-02 or 6.80%

The result for Level 4 is the human error probability in the pre-accidental condition related to the fact the valves were left closed, which is considered as the TMI initiator event in a number of NRC reports.

The analysis of the procedures presented above, taking the emergency feedwater system as an example, can be applied to any other human errors that have occurred in TMI.

6. Conclusions

- Although identified by the licensee, the need of design modification in the electrical system, specifically related to the condensate pump instrumentation, has never been implemented by the utility (NUREG-0600, 1979). Moreover, there were other design deficiencies in the condensate and feedwater systems, as well as leaking in the pressurizer valve and ergonomical deficiencies in the man-machine interface of the control room. These were the main technical causes that led TMI staff to operating the plant within an inappropriated technical and organizational condition.
- It should be emphasized that in a nuclear power plant, the heat generation process by means of nuclear fission is extremely dynamic. Due to this, tasks to be accomplished by the operators under extreme unusual conditions, as plant deviation identification, diagnosis and decision making need to be done very fast. During the course of TMI accident, operators were not able to successfully cope with these tasks, because they were previously stressed, striving to operate the plant, which had already deviated from required standards.
- We have shown that the combination of ATHEANA (NUREG/CR-6350, 1996 and NUREG-1624, 2000) and THERP (NUREG/CR-1278, 1983) methodologies to create an innovative intermediate methodology is very useful, concerning operational context and error mechanisms. It provides the expert with a broader overview of the plant, which allows a more realistic prediction of events that may occur.

7. Recommendations

- Based on the conclusions described above, the socio-technical context should be integrated into the HRA.
- The human reliability analysts should be trained to develop technical expertise, in order to be able to psychologic, anthropologic and ergonomically analyze the possible accident sequences.
- The Human Reliability Engineering analysis needs to overcome the Cartesian paradigm in order to achieve the socio-technical context.
- The pre-accidental factors that modify the HEP probabilities should be modeled in pre-accidental contexts.
- Modeling and implementing these factors are the most important tasks of the use of the innovative methodology, originated from THERP (NUREG/CR-1278, 1983) and ATHEANA (NUREG/CR-6350, 1996 and NUREG-1624, 2000), which the HRA should adopt.
- It is also worth mentioning that in HRA, plant contexts such as design issues and maintenance policies, which include ergonomic and organizational aspects, are central to obtaining good human behavior performance.

8. References

NUREG-75/014, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400. U. S. Nuclear Regulatory Commission, Washington, DC, October 1975.

NUREG-0600, Investigation into the March 28, 1979 Three Mile Island Accident by Office of Inspection and Enforcement. U.S. Nuclear Regulatory Commission: Washington, DC, July 1979.

NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications Final Report. U.S. Nuclear Regulatory Commission: Washington, DC, August 1983.

NUREG-1624, A Technique for Human Event Analysis. U.S. Nuclear Regulatory Commission: Washington, DC, May 2000.

NUREG/CR-5455, Development of the NRC's Human Performance Investigation Process (HPIP). U.S. Nuclear Regulatory Commission: Washington, DC, October 1993.

NUREG/CR-6350, A Technique for Human Error Analysis. U.S. Nuclear Regulatory Commission: Washington, DC, May 1996.

Servan-Schreiber, D., The Instinct to Heal: Curing Depression, Anxiety and Stress Without Drugs and Without Talk Therapy. Rodale Inc, Emmaus, Pennsylvania, 2004.