

## Research Article

# A THERP/ATHEANA Analysis of the Latent Operator Error in Leaving EFW Valves Closed in the TMI-2 Accident

**Renato A. Fonseca,<sup>1</sup> Antonio Carlos M. Alvim,<sup>2</sup> Paulo Fernando F. Frutuoso e Melo,<sup>2</sup> and Marco Antonio B. Alvarenga<sup>1</sup>**

<sup>1</sup> Brazilian Nuclear Energy Commission, 22290-901 Rio de Janeiro, RJ, Brazil

<sup>2</sup> COPPE—Graduate Program of Nuclear Engineering, Federal University of Rio de Janeiro, 21941-914 Rio de Janeiro, RJ, Brazil

Correspondence should be addressed to Antonio Carlos M. Alvim; [aalvim@gmail.com](mailto:aalvim@gmail.com)

Received 6 November 2012; Revised 7 March 2013; Accepted 10 March 2013

Academic Editor: Alejandro Clausse

Copyright © 2013 Renato A. Fonseca et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This paper aims at performing a human reliability analysis using THERP (Technique for Human Error Prediction) and ATHEANA (Technique for Human Error Analysis) to develop a qualitative and quantitative analysis of the latent operator error in leaving EFW (emergency feed-water) valves closed in the TMI-2 accident. The accident analysis has revealed a series of unsafe actions that resulted in permanent loss of the unit. The integration between THERP and ATHEANA is developed in a way such as to allow a better understanding of the influence of operational context on human errors. This integration provides also, as a result, an intermediate method with the following features: (1) it allows the analysis of the action arising from the plant operational context upon the operator (as in ATHEANA), (2) it determines, as a consequence from the prior analysis, the aspects that most influence the context, and (3) it allows the change of these aspects into factors that adjust human error probabilities (as in THERP). This integration provides a more realistic and comprehensive modeling of accident sequences by considering preaccidental and postaccidental contexts, which, in turn, can contribute to more realistic PSA (Probabilistic Safety Assessment) evaluations and decision making.

## 1. Introduction

The TMI accident is one of the most used accidents to demonstrate the application of the concepts of human reliability analysis [1–4]. It became also a benchmark scenario to test new HRA techniques, in view of latent and active failures [5] that contributed to the arising of human errors, as well as the complexity involved in the interaction between them. As a consequence of the TMI accident, many modifications have been implemented into nuclear power plants all over the world. However, despite these modifications, many human failures continue to occur [1, 2].

In the well-known WASH 1400 report [6], human reliability analysis (HRA) received a formal treatment. Experts on the nuclear engineering field are the precursors of HRA studies. The first steps taken by these experts were to include psychological and physiological stressors, organizational

factors, and situational, task, and equipment characteristics into HRA studies. One of the first techniques developed for human reliability analysis under the context of probabilistic safety assessment was THERP (Technique for Human Error Rate Prediction) [2, 7]. THERP has been extensively used in probabilistic safety assessments in the nuclear field, along with many applications to other probabilistic safety studies as, for example, in the chemical and oil industries. THERP is considered a first generation HRA technique because its quantification tables of human errors are based on a taxonomy that does not take human error mechanisms into account and also on the level of characterization of the context in which errors take place.

To overcome the disadvantages and deficiencies discussed before, second generation HRA techniques have been developed, among which we will discuss ATHEANA (Technique for Human Event Analysis) [1, 2]. ATHEANA originated

from a study accomplished by the Nuclear Regulatory Commission (NRC) Department of Analysis and Evaluation of Operational Data (AEOD) in 1995. AEOD analyzed various serious incidents that happened and it was verified that some operator actions not included in the procedures, which jeopardized the plant operational structure and worsened the accident conditions, were not represented, treated, and considered in PSA studies, as they should be.

ATHEANA treats the error-forcing context due to the combination of plant conditions and other influences (preinitiators), which can contribute to human failures. It also treats error types, error mechanisms, unsafe actions, performance shaping factors of human actions, and mental models (tendencies) of operators by using informal rules, as a function of scenario operational characteristics and operational behavior of process variables.

It accomplishes an analysis of human error perspectives, by means of a retrospective analysis of significant events that already happened and a prospective analysis that identifies potential operator errors during plant operation.

It also verifies existing vulnerabilities in operator training processes and their qualification exams.

ATHEANA makes possible a structured and differentiated analysis due to the use and integration of knowledge and experiences in PSA, engineering, human factors, and cognitive psychology. It also considers the specific plant information and experiences arising from significant accident analyses.

This paper discusses the possibility of integrating preaccidental and post-accidental contexts of the Three Mile Island, Unit 2 accident, which can make the accident analysis more comprehensive and realistic.

In the preaccidental context, a qualitative analysis is performed, by means of the use of ATHEANA, which considers the essential factors for the TMI plant modeling. On the other hand, THERP is quantitatively applied to the postaccidental context, through its HEP tables. It should be emphasized that the results of the preaccidental context are linked to the post-accidental ones.

The link between both techniques is provided through a qualitative analysis of the plant context developed within ATHEANA, which allows the introduction of correction factors into the human error probabilities used in THERP. This correction is performed with the inclusion of the context preaccidental conditions upon operators, which gives the condition, after the qualitative analysis, of choosing the factors to correct THERP's tables. This link breaks the simplified approach of reasoning with failure or success modeled in the event trees of THERP. The analysis of preaccidental conditions implies the consideration of the precursors that contribute to the initiation of human failure and allows working within the good practices of human reliability analysis [8].

This paper is organized as follows. Section 2 presents limitations inherent to THERP that can be overcome by ATHEANA, thus explaining its joint use, and also focuses on the merged THERP-ATHEANA model itself. Section 3 presents the TMI preaccidental analysis. Finally, conclusions and recommendations are the subject of Section 4.

## 2. Human Reliability Analysis Modeling

Among THERP disadvantages and deficiencies, one may refer to the following:

- (i) THERP has an enormous discrepancy in the socio-technical profile of its data tables [1, 9].
- (ii) In spite of the incorporated modifications, doubts on Human Error Probability (HEP) data still remain, especially due to the limited focus on external error (omission and commission errors, the latter only in the level of slips, in other words, in the perceptual-motor level) [5].
- (iii) Its approach is still based on the stimulus-organism-response (SOR) paradigm (introduced by R. S. Woodworth in 1929 to describe his functionalist approach to psychology and to stress its difference from the strictly stimulus-response (SR) approach of behaviorists), which is no more accepted in psychology [10, 11].
- (iv) It does not properly treat the cognitive process that cannot be reduced merely to commission and omission errors. The cognitive process involves information processing with the following phases: detection and perception, decision making, and response selection, execution of actions, and control of attention resources, being furthermore influenced by the context [10, 11].
- (v) It does not consider the factors linked to the plant context that can induce humans to make errors (error-forcing context), including plant organizational factors [9–12].
- (vi) The training process is treated summarily, showing a mechanistic view of human beings [1].
- (vii) HEP tables are focused on tasks; therefore, human errors are treated in a standardized way (error in the choice of a command, error in the reading of an instrument, error in the checking of an action, etc.), erroneously reflecting a mechanistic relationship between man and the plant, and thus THERP is not rich enough to capture the man-system interaction dynamics and complexity [9].
- (viii) It does not take into account the context of tasks in a comprehensive way, because it works with a few performance shaping factors (considered the most important ones). The development of the context through the interaction between performance shaping factors and plant special conditions (operation, maintenance, etc.) is not evaluated, as it would be in a human reliability technique of second generation, such as, for example ATHEANA [1].

ATHEANA presents some advantages, as stated next.

- (i) The retrospective analysis of events is of great usefulness in several situations and can be used to aid in understanding causes of the occurrence of specific events and what measures can be taken in order to preclude them.

- (ii) The retrospective analysis aids in the analysis of human actions, including the development of general or specific perceptions of the plant, recommendations to improve its potential, and information to give support to the accomplishment of PSA and HRA. It also helps in the performance of accident investigations and root-cause analyses.
- (iii) The prospective analysis of events integrates the pertinent subjects into PSA and HRA, identifies human failure events and important unsafe actions (basis to identify the reasons behind event occurrence), and quantifies error-forcing contexts and probabilities of unsafe actions, given the contexts.
- (iv) The prospective analysis aids in the characterization of human behavior, giving more options to manage plant risks by means of better knowledge of the implicit causes of human error and the vulnerabilities not noticed in the operator's behavior, regarding automatic devices in specific contexts.
- (v) The prospective analysis concerning training identifies the weak points not explored in the requirements of training programs, the complementary scenarios in the simulator training exercises, and the necessary improvements of operator's qualification exams.
- (vi) It integrates the progresses of psychology and engineering into modeling, and actual plant conditions to PSA.
- (vii) It presents tables that relate error causes to its manifestations (operational activities). Consequently, error causes in subsequent tables are linked to error mechanisms, error types and performance shaping factors (PSFs), although the proposed quantification has not as yet been implemented.
- (viii) Regarding PSA, the model is updated—it does not consider the stimulus-organism-response (SOR) paradigm, and it agrees with modern progresses of cognitive sciences.
- (ix) Concerning PSA, it accomplishes a deeper qualitative analysis of the sociotechnical context for operators, because, for example, it treats the error-forcing context and its relationships with the cognitive process.
- (x) ATHEANA presents one main disadvantage: its quantitative analysis of human error probabilities is not satisfactorily developed yet.

ATHEANA states a variety of paths to be used in order to perform a PSA aiming at building a structure of logical steps. 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 time and causal aspects, although during the accident sequence course they do not precisely define the events related to human behavior.

In addition to that limitation, other issues should be considered when it comes to logical models as follows.

- (i) Human failure events do not clearly indicate the possible influences of operator performance.
- (ii) Instrumentation failures that can impact on operator response are not well specified.
- (iii) Some of the plant conditions are not adequately characterized with respect to their influences on operator performance.
- (iv) Some issues that can influence the error-forcing context, which can lead to an operator error, are not taken into account.

However, ATHEANA deals with the above-mentioned limitations and clearly addresses the accident modeling considering the plant preaccidental context. It is important to notice that this analysis enables a better understanding of the applicability of THERP tables.

In this work, ATHEANA is integrated into THERP, making it possible to quantify the probability of human error. This integration establishes an intermediate methodology which is the outcome of an innovative approach in the context of human reliability analysis.

Plant conditions represent the (operational and organizational) factors that can influence plant operator performance. They characterize the circumstances in which operator activities are affected by performance shaping factors. These factors include plant configuration aspects, process parameters, and off-nominal conditions.

Performance shaping factors represent the context influences that may affect human behavior. Due to that, a human failure event can occur. Many of the performance shaping factors are identified in [13]: stress, organizational factors, environmental conditions, training, procedures, and human-system interfaces. Some of them are linked to design features, as in the case of the human-system interface; others are linked to maintenance aspects, as in the case of maintenance procedures [13, 14].

The error-forcing context represents the combination of performance shaping factors effects and plant conditions that together create a favorable situation for the occurrence of human errors.

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. The error mechanisms can appear during the following situations: detection, evaluation, and response planning and implementation.

Unsafe actions represent actions inappropriately taken by the plant personnel or actions not taken when necessary, resulting in degradation of the plant safety condition. ATHEANA assumes that significant unsafe actions occur, as a result of the combination of influences associated with such plant conditions and psychological conditions that trigger error mechanisms in plant personnel. There are specific error mechanisms for each type of human error (slips, lapses, and mistakes) and each one can trigger an unsafe action [14]. The error mechanisms are internal cognitive processes in human reasoning, while an unsafe action is the result of human error in the external world.

Human errors are characterized as divergences between actions actually taken and the ones that should have been taken.

The result of an unsafe action is the failure of a safety function with the consequent failure of a system and/or component, which results in a worsened plant condition. In HRA, these failures are modeled by means of failure trees or event trees with human failure events (HFEs). A HFE can be classified as a commission error or an omission error.

Plant scenarios comprise minimum descriptions of the plant context required to develop the PSA model, defining the appropriate human failure events.

### 3. Preaccidental Analysis of the TMI Latent Operator Error in Leaving EFW Valves Closed

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

In the preaccidental context, it is necessary to analyze the plant and check its degree of availability and reliability. The type of maintenance, plant technology, interpersonal relationships, organizational ethics, and so forth should also be checked. In this work, the preaccidental analysis is based on [15].

*3.1. System Failures in the Preaccidental Context.* In the preaccidental 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 [15].

One or more of the pressurizer relief valves were leaking into the reactor coolant drain tank at approximately 6 gpm. This continuous leakage caused boron concentration to continuously increase in the pressurizer. The relief valve exhaust continuously indicated approximately 180–200°F (exceeding the normal 130°F) due to leakage.

The condensate system includes a full-flow polisher (demineralizer) system to provide continuous demineralization of the condensate water supplied to the feed-water system and the once-through steam generator. A full-flow motor-operated bypass valve is provided around the polishers which can be operated from the control room. This valve does not automatically open upon polisher system malfunctions (high differential pressure to the condensate booster pump suction). Prior to the accident, operators were working to transfer resin from polisher tank number 7 to the resin regeneration tank.

A licensee concern as to the capacity of the air system was recognized early in the construction/preoperational phase of TMI-2. The solution of the capacity problem was cross-connecting the station service air system to the instrument air system as a normal mode of operating the two systems. Discussions with the licensee personnel indicated that there was

a pending change that would isolate part of the station service air system. This change and its status were not pursued for details. The air supply operation mode on March 28, 1979, was the cross-connected system.

Discussion with a licensee engineer indicated that he had also found that the solenoid switch wiring for the polisher valve controls was not in accordance with drawings in at least two polisher units. This could affect the status of the valves on power failure. He also stated that there was a wiring error related to the condensate/condensate booster pump auto/manual switch such that, on a trip of condensate booster pump, its paired condensate pump would trip. This wiring error was isolated to the A pump pair so that condensate B pump would remain on line when its paired booster pump tripped.

*3.2. Preaccidental Context.* In the preaccidental context, the qualitative aspects of ATHEANA are integrated into THERP. Based on that, the tables that show HEPs, presented in THERP, can deal with the preaccidental context. This analysis demonstrates that THERP can still be considered a useful tool.

Remarks on plant conditions include [15] the following: (a) the plant configuration has indicated the existence of operational problems in the reactor cooling system, condensate system, feed-water system, compressed air system and electrical system; (b) plant parameters such as temperature, pressure and coolant inventory related to the reactor cooling system were not in compliance with standards; (c) plant conditions related to leak through the pressurizer safety valve together with the above-mentioned process parameters were not in compliance with safety principles.

Concerning performance shaping factors, there are aspects to be mentioned that concern organizational factors, job instructions, task characteristics, and stress.

In what concerns 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 [15].

Concerning job instructions, the preaccidental context had shown a situation where procedures and standards were not met. Moreover, working conditions were inadequate or the plant staff was not sufficiently trained to understand the plant context. It should be emphasized that the NUREG-0600 report [15] states that the plant staff had already, at the time, enough operational experience.

Critical tasks need to be correctly interpreted by the control room personnel, who should have deep plant knowledge. They should also be able to anticipate events and establish a safe action based on the plant context. In the TMI accident, human performance in the preaccidental and post-accidental contexts contributed to worsen the accident course.

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 an HE occurrence was only a matter of time.



The error mechanism that most influenced the preaccidental context was the previous incorrect assessment phase (application of incorrect rules and misapplication of correct rules). Moreover, another error mechanism of the 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.

In the preaccidental context, unsafe actions are related to inappropriate actions such as (a) emergency feed-water block valves left shut [15], (b) use of instrument air to try to release blocked resin in the transfer line [15], and (c) high pressure injection throttling to prevent the pressurizer from becoming solid [15].

Failures that have occurred in the plant (emergency feed-water block valves were closed and pressurizer relief valve did not close after opening) have also induced the plant staff to commit HEs.

**3.3. Analysis of the Preaccidental Factors.** Preaccidental factors originate from the integration of THERP and ATHEANA. This analysis comprises mostly the verification of plant characteristics, as well as performance shaping factors (PSF) that have occurred prior to the event, which could influence the course of an incident or an accident. Each plant context is subdivided into a few items 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.

The following list of characteristics found can be applied to any nuclear power plant. There is no restriction to adding another characteristic to this list by the human reliability analyst or by the plant personnel.

Some PSFs are linked to the organizational culture and to how groups interact with each other, for example, the engineering, maintenance, and operational staff [13]. In this case we must evaluate the specific situation for each plant by means of the data mined in its operational experience, which provides a statistics of root causes linked to organizational factors to quantify this kind of PSF. In the following we describe how these PSFs can be better treated in HRA.

Relevant characteristics concerning the TMI design are as follows. (a) It has been adequately developed, (b) presented failures that could be corrected with the implementation of minor modifications, (c) presented failures that compromise its operation and safety, (d) presented failures that prevented its proper operation and compromises safety, (e) presented failures on its basis.

Concerning TMI maintenance, it was (a) carried out with continuously monitored appropriate criteria, (b) carried out with appropriate criteria without being monitored, (c) of preventive type, (d) of opportunity type, (e) carried out under emergency conditions.

There are distinct technological updating levels concerning plant design. The plant may be considered (a) up to date, (b) slightly behind of up-to-date engineering standards, (c) considerably behind of up-to-date engineering standards, (d) becoming obsolete, (e) already obsolete.

Concerning plant design, there are different ergonomic scenarios (a) being ergonomically adequate, (b) needs ergonomic adjustments, (c) needs ergonomic restructuring, (d) needs an ergonomic design.

Concerning equipment technical specifications, four possibilities were taken into account (a) specification were in accordance with design and required quality standards, (b) specifications were in accordance with design but not with required quality standards, (c) specifications were neither in compliance with design nor with required quality standards, (d) there were no specifications for the equipment.

There are distinct types of human resources management, as, for example, (a) excellent, (b) satisfactory, (c) below satisfactory, and (d) needs a change in its policy.

**3.4. Operational Quality Levels and Preaccidental Factors.** Table 1 displays the operational quality levels and preaccidental factors.

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

**3.5. Event Tree of the Preaccidental Context.** There was a HE in the TMI preaccidental context: due to negligence, EF-V-12A and EF-V-12B valves had been left closed after the emergency feed-water valve test [15]. Should the emergency feed-water system be required under operational incident conditions, it would have been unavailable, unless the valves were manually opened [15]. The calculation of HEP related to leaving valves closed can be done as discussed next.

Task A comprises the emergency feed-water valve test. The HEP for this task, which is  $1.0E-02$ , is displayed in Table 20-6 of THERP [7]. The HE for Task A lies in the fact that the crew forgot to open the feed-water valves after the test.

Task B comprises the verification of the valves' original positions after the test. The HEP for this task, which is  $1.0E-01$ , is displayed on Table 20-22 of THERP [7]. The HE for Task B is the lack of verification whether the valves have been left closed.

To calculate the HEP, the level of dependence between test and inspection teams should be taken into account. In order to include that dependence, a few parameters need necessarily to be considered: (a) conservatively take into account a low level of dependence between teams (test and inspection) in Task B; (b) take into account, as a conservative approach, a high level of dependence between the acts of closing both valves. If a valve has been left closed, it is very likely that the other valve will also be left in the same position.

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

Capital letters represent error probabilities, whereas small letters stand for success probabilities. The HEP of EF-V-12A

TABLE 1: Operational levels based on pre-accidental factors.

Operational level 1
Plant is operating under adequate operational and safety standards.
Preaccidental factor = 1 (skilled operator)
Preaccidental factor = 1 (novice)
Operational level 2
Plant requires few operational reviews without which safety will be jeopardized in the long run.
Preaccidental factor = 1 (skilled operator)
Preaccidental factor = 2 (novice)
Operational level 3
Plant requires operational reviews without which safety will be jeopardized in the medium run.
Preaccidental factor = 2 (skilled operators)
Preaccidental factor = 4 (novice)
Operational level 4
Plant requires shutdown to allow operational safety review.
Preaccidental factor = 5 (skilled operators)
Preaccidental 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)

valve left closed is  $1.45E - 03$ , as shown in Figure 1, which is the same probability for leaving the EF-V-12B valve closed, considering a level of independence between them.

Both EF-V-12B and EF-V-12A valves have been left closed due to a high dependency between teams, which is shown in Figure 2. This figure 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, whose value is modified due to a 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 from Figure 2.

The task involves the above-mentioned test with an 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 of THERP's Table 20-20 [4, 7]. Thus, it is possible

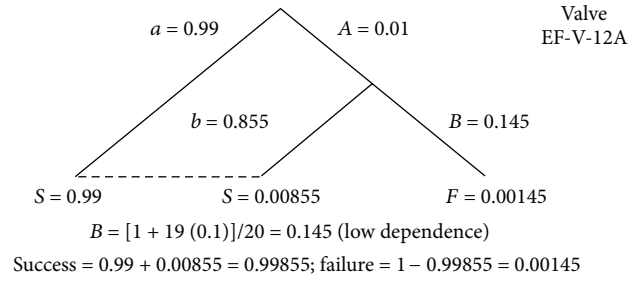


FIGURE 1: Low dependency between teams in Task B.

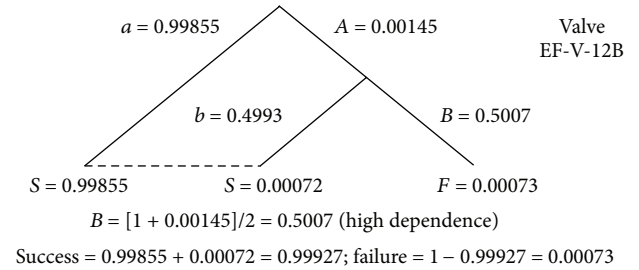


FIGURE 2: Dependence between teams that operate EF-V-12A and EF-V-12B valves.

to calculate the uncertainty limits: lower bound =  $7.3E - 05$ ; upper bound =  $7.3E - 03$ .

The TMI preaccidental scenario is of operational level 4, as shown in Table 1. This means that any HEP, either in the preaccidental or in the post-accidental context, can be obtained by means of the multiplication by a factor of 5 in the case of a skilled operator and by a factor of 10 for a novice one.

Task A (HEP =  $1.0E - 02$ ) gives a probability of  $5.0E - 02$ , while Task B (HEP =  $1.0E - 01$ ) gives a probability of  $5.0E - 01$ . Figures 3 and 4 show the event trees and the HEP-related calculations, considering dependences.

The task involves the above-mentioned system test with an associated error probability of  $1.35E - 02$ , which is greater than  $1.0E - 02$ . Therefore, the associated error factor is 5, which can be seen on item 3 of THERP's Table 20-20 [7]. 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. HEP results obtained for level 1 are related to nominal values from THERP [7]. On the other hand, HEP results obtained for level 4 have the HEP values multiplied by a preaccidental factor of 5. The upper bound limit is adopted for both levels 1 and 4 due to the adopted conservative approach:

- (i) HEP for level 1:  $7.3E - 03$  or 0.73%.
- (ii) HEP for level 4:  $6.8E - 02$  or 6.80%.

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

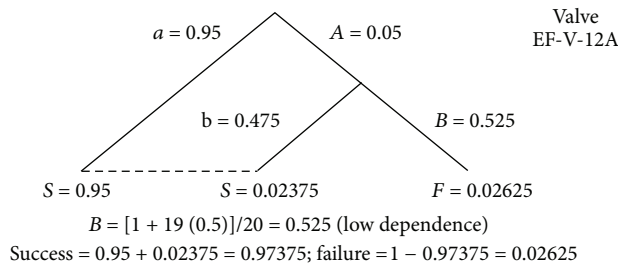


FIGURE 3: Dependence between teams in Task B.

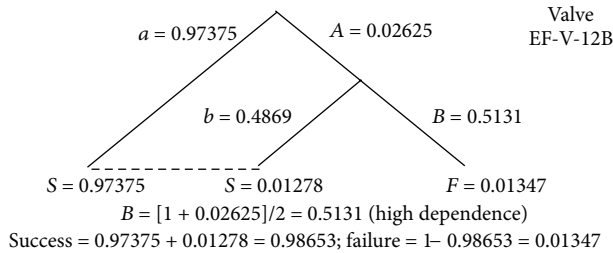


FIGURE 4: Dependence between teams that operate EF-V-12A and EF-V-12B valves.

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

#### 4. Conclusions and Recommendations

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 [16]. Moreover, there were other design deficiencies in the condensate and feed-water systems, as well as a leaking in the pressurizer valve and ergonomic deficiencies in the man-machine interface of the control room. These were the main technical causes that led the TMI staff to operate the plant within an inappropriate technical and organizational condition.

We have shown that the combination of ATHEANA and THERP can be very useful, concerning the operational context and error mechanisms. It provides the expert with a broader plant overview, which allows a more realistic prediction of events that might occur. This may contribute to more realistic PSAs in the context of decision making.

Based on the conclusions described above, the socio-technical context should be integrated into nuclear power plant HRA. This poses new challenges to HRA. This means, for example, consideration of organizational features in an integrated fashion, not to violate the concept of a socio-technical system [17, 18].

Human reliability engineering analysis needs to overcome the Cartesian paradigm in order to achieve the socio-technical context. This means that human error mechanisms are triggered by external factors. The Cartesian paradigm states that mind and body are dissociated from each other.

The preaccidental factors that modify the HEP probabilities should be modeled in preaccidental contexts. Modeling and implementing these factors are the most important tasks of the use of the proposed approach, originated from THERP and ATHEANA.

It is also worth mentioning that we have chosen a preinitiator error for discussion in this paper but it is intended to apply this approach to errors in the accident sequence (related to decision making) to evaluate further the approach discussed here.

Finally, it is interesting to note that even considering natural phenomena (earthquakes, tsunamis, etc.), all inferences and recommendations achieved in this paper can be applied to the Fukushima accident. Reference [19] corroborates the last sentence because it concluded that the accident causes residing in organizational factors rather than on individual skills. These factors influenced both preaccident and post-accident tasks.

#### References

- [1] NRC, "A technique for human event analysis," NUREG-1624, US Nuclear Regulatory Commission, Washington, DC, USA, 2000.
- [2] NRC, "A technique for human error analysis," NUREG/CR-6350, U.S. Nuclear Regulatory Commission, Washington, DC, USA, 1996.
- [3] B. Reer, "Review of advances in human reliability analysis of errors of commission—part 2: EOC quantification," *Reliability Engineering and System Safety*, vol. 93, no. 8, pp. 1105–1122, 2008.
- [4] P. Le Bot, "Human reliability data, human error and accident models—Illustration through the Three Mile Island accident analysis," *Reliability Engineering and System Safety*, vol. 83, no. 2, pp. 153–167, 2004.
- [5] J. Reason, *Human Error*, Cambridge University Press, Cambridge, UK, 1990.
- [6] NRC, "Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400. NUREG-75/014, US Nuclear Regulatory Commission, Washington, DC, USA, 1975.
- [7] A. D. Swain and D. Guttman, "Handbook of human reliability analysis with emphasis on nuclear power plant applications," NUREG/CR-1278, US Nuclear Regulatory Commission, Washington, DC, USA, 1983.
- [8] NRC, "Evaluation of human reliability analysis methods against good practices," NUREG-1842, US Nuclear Regulatory Commission, Washington, DC, USA, 2006.
- [9] E. Hollnagel, *Cognitive Reliability and Error Analysis Method (CREAM)*, Elsevier, Oxford, UK, 1998.
- [10] E. Hollnagel, "The reliability of man-machine interaction," *Reliability Engineering and System Safety*, vol. 38, no. 1-2, pp. 81–89, 1992.
- [11] E. Hollnagel, *Human Reliability Analysis: Context and Control*, Academic Press, London, UK, 1993.
- [12] E. Hollnagel, "Reliability analysis and operator modelling," *Reliability Engineering and System Safety*, vol. 52, no. 3, pp. 327–337, 1996.
- [13] NRC, "Development of the NRC's Human Performance Investigation Process (HPIP)," NUREG/CR-5455, US Nuclear Regulatory Commission, Washington, DC, USA, 1993.

- [14] NRC, “The SPAR-H human reliability analysis method,” NUREG/CR-6883, US Nuclear Regulatory Commission, Washington, DC, USA, 2005.
- [15] NRC, “Investigation into the March 28, 1979 three mile island accident by office of inspection and enforcement,” NUREG-0600, US Nuclear Regulatory Commission, Washington, DC, USA, 1979.
- [16] J. W. Kim, W. Jung, and J. Park, “A systematic approach to analysing errors of commission from diagnosis failure in accident progression,” *Reliability Engineering and System Safety*, vol. 89, no. 2, pp. 137–150, 2005.
- [17] Z. Mohaghegh, R. Kazemi, and A. Mosleh, “Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: a hybrid technique formalization,” *Reliability Engineering and System Safety*, vol. 94, no. 5, pp. 1000–1018, 2009.
- [18] K. M. Groth and A. Mosleh, “A data-informed PIF hierarchy for model-based human reliability analysis,” *Reliability Engineering and System Safety*, vol. 108, pp. 154–174, 2012.
- [19] The National Diet of Japan, *The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission*, Fukushima Nuclear Accident Independent Investigation Commission (NAIIC), Tokyo, Japan, 2012.



