BNL-NUREG-63257

CONF- 960912--39

A PROCESS FOR APPLICATION OF ATHEANA

- A NEW HRA METHOD

Gareth W. Parry
NUS
910 Clopper Road
Gaithersburg, Md., 20878
(301) 258 2536

Dennis C. Bley
Buttonwood Consulting
11738 English Mill Court
Oakton, Va. 22124
(703) 648 2545

Susan E. Cooper
SAIC
11251 Roger Bacon Drive
Reston, Va. 22090
(703) 318 4635

John Wreathall
John Wreathall and Co.
4157 MacDuff Way
Dublin, Oh. 43016
(614) 791 9264

William J. Luckas,
John H. Taylor
BNL
Upton, NY 11973
(516) 344 7005

Catherine M. Thompson,
Ann M. Ramey-Smith
USNRC
Washington, DC 20555
(301) 415 6981/6877

ABSTRACT

This paper describes the analytical process for the application of ATHEANA, a new approach to the performance of human reliability analysis as part of a PRA. This new method, unlike existing methods, is based upon an understanding of the reasons why people make errors, and was developed primarily to address the analysis of errors of commission.

I. INTRODUCTION

This paper presents an outline of an analytical process for performing a human reliability analysis (HRA) in the context of a probabilistic risk assessment (PRA), that addresses the major deficiencies of current HRA methods, and, in particular, provides an approach to the analysis of errors of commission. This analytical process has been developed using the concepts captured in the multidisciplinary framework described in NUREG/CR-6265[1], and supplemented with the experience obtained from the analysis of historical events at low power and shutdown, as described in NUREG/CR-6093[2]. Both of these documents are earlier products of the project initiated by U.S. Nuclear Regulatory Commission in response to the recognized need for an improved, more realistic, approach to the modeling of human-system interactions. The framework recognizes the need to bring together the disciplines of behavioral science, cognitive psychology, and systems analysis, as well as input from plant operations, in order to capture realistically the human-systems interactions and their impact on safety. The analytical process is the application phase of a new approach to human reliability analysis. This approach, called ATHEANA[3] (A Technique for Human Error Analysis), is based on an understanding of why human-system interaction failures occur, rather than on a behavioral, phenomenological description of operator responses, and represents a fundamental change in the approach to human reliability analysis. Section II of this paper presents an overview of the ATHEANA method, and Section III describes the application process.

II. OVERVIEW OF THE ATHEANA METHOD

There are important human performance issues which are addressed in the ATHEANA HRA method to make the required improvements in HRA/PRA applications. The issues which represent the largest departures from current HRA methods all stem from the need to better predict and reflect the "real world" nature of failures in human-system interactions, as illustrated by past operational events. Real operational events frequently include post-accident errors of commission, which are minimally addressed in current HRA/PRAs. The occurrence of an error of commission is strongly influenced by the specific context of the event (i.e., plant conditions and performance shaping factors). This specific context of an event frequently departs from the nominal plant conditions assumed by PRA and HRA analysts to represent the plant conditions during off-normal incidents.

Consequently, the HRA modeling approach adopted for ATHEANA is a significant shift from current approaches. In particular, to be consistent with operational experience, the fundamental premise of ATHEANA is that significant post-accident human failure events, especially errors of commission, represent situations in which the context of an event (plant conditions, PSFs) virtually forces operators to fail. It is this focus on the error-forcing context which distinguishes ATHEANA from other HRA methods.

The ATHEANA modeling approach involves more than simply a new quantification model. Included in ATHEANA is a better, more comprehensive approach to the identification and definition of appropriate human failure events (HFEs), and the placement of these human failure events in the PRA model. The guidance on how to search for the HFEs is based on an understanding of the causes of human failures as indicated above.

In applying ATHEANA to a PRA, the representation of post-accident HFEs which are errors of commission will be similar to the representation of errors of omission already addressed by existing HRA methods, in that they will be identified and defined in terms of failure modes of plant functions, systems, or components. However, errors of omission (EOOs) result from failures of manual operator actions to initiate or change the state of plant equipment. Therefore, EOO definitions typically are phrased as "operator fails to start pumps", for example. Errors of commission, on the other hand, result from specific actions on the part of the operators. Generally, post-accident errors of commission result from one of the following ways by which operators fail plant functions, systems, or components:

- by turning off running equipment;
- by bypassing signals for automatically starting equipment;
- by changing the plant configuration such that interlocks that are designed to prevent equipment damage are defeated; and
- by excessive depletion or diversion of plant resources (e.g., water sources).

In a PRA model, only the most significant and most likely HFEs need be included. Identification of the most likely is based on an understanding of the causes of error.

An HFE may result from one of several unsafe actions[1]. Application of ATHEANA involves, for each HFE, the identification and definition of unsafe actions and associated error-forcing contexts (EFCs). The identified error-forcing contexts (i.e., plant conditions and associated PSFs), and their underlying error mechanisms, are the means of characterizing the causes of human failures. An unsafe action could be the result of one of several different causes.

Implicit in the definition of the HFEs and unsafe actions is the recognition that, because of the nature of nuclear power plant operational characteristics, there is generally time for the operators to monitor the changes they have initiated, which allows them opportunities to recognize and correct errors. Thus, the unsafe action is a result of an error and a failure to correct that error before the failure associated with the PRA basic event occurs. Therefore, the error forcing context associated with an unsafe action must address the factors that impact both the initial error and the failure to recover.

In the application of ATHEANA, the prioritization of HFEs will be based on the probabilities of the contributing unsafe actions, and these in turn will be based on the probabilities of the associated EFCs. Quantification of the probabilities of corresponding HFEs will be based upon estimates of how likely or frequently the plant conditions and PSFs which comprise the error-forcing contexts occur, rather than upon assumptions of randomly occurring human failures. Therefore, quantification of an HFE using ATHEANA is based upon an understanding of the following:

- what unsafe action(s) can result in the HFE whose probability is being quantified?
- what error-forcing context(s) can result in the unsafe action(s) comprising the HFE?
- how likely are these error-forcing contexts to occur?

As discussed above, there are two sets of EFC elements to consider: those associated with the initial error, and those that impact the potential for recovery. There may be common EFC elements between the two sets, and therefore the EFCs for a given unsafe action will be given by the union of the two sets of elements.

ATHEANA will be supported by two documents. The first, called the Frame of Reference Manual contains the knowledge required to apply the method. A related paper presented at this conference describes the Frame of Reference Manual[4]. The second is called The Implementation Guidelines, and describes how to apply this knowledge in a plant specific manner. The underlying analytical process for application of ATHEANA is described below.

DISCLAIMER

III. THE ATHEANA PROCESS

The ATHEANA application process has been discussed in detail in Reference 5. Since publication of that document, considerable progress has been made on the development of the Frame of Reference Manual, and the discussion of the process presented in this paper reflects this progress. The general structure of the process, captured in Figure 1, "Flow diagram of analytical procedure", taken from Reference 5, is still valid. Five tasks are identified. These are:

- Identification of the candidate human failure events to be modeled;
- Identification of potentially important types of unsafe actions that could cause each HFE;
- For each type of unsafe action, identification of the most significant reasons for that type of unsafe action to occur, and for each type of unsafe action and its associated reason, identification of the potentially significant error-forcing contexts;
- For each type of unsafe action and its associated reason, estimate the likelihoods of the error-forcing contexts and the consequential probabilities of the unsafe actions; and
- For each HFE, sum the likelihoods of the error-forcing contexts and consequential probabilities of the unsafe actions for all potentially important types of unsafe actions that could cause the HFE.

Presented in this way, the process appears to be somewhat open-ended, since there is potentially a very large number of combinations of HFEs, unsafe actions, and error-forcing contexts that could contribute to the occurrence of a severe accident. However, the ATHEANA method Implementation Guidelines will incorporate detailed guidance on how to prioritize and/or screen the HFEs and unsafe actions for the most significant. At the highest level, the following general prioritization criterion is proposed:

- The unsafe actions of most interest are those that are taken on a rational (if incorrect) basis; that is, irrational, spontaneous, and arbitrary actions are not considered.

This section discusses how the information presented in the Frame of Reference Manual will be used in the five tasks identified above and in Figure 1, and how the high level criterion is implemented.

Task 1: Familiarization with PRA Model and Accident Scenarios

It is assumed in this paper that the analysis starts with an existing PRA. To analyze the human-system interactions within the context of that model it is necessary to become familiar with the definitions of all the elements of that model, and with the accident scenarios identified. It is also essential to understand the assumptions underlying the PRA model. Clearly, a key element in performing an HRA is to identify the role of the operating crew in mitigating, or controlling the progress of the accidents represented by the scenarios. It is essential to become familiar with the set of applicable procedures, and to understand which, and under what plant conditions, procedures are required. It is also necessary for the human reliability analyst to develop a clear picture of how the plant responds to the functional failures and operator actions represented in the scenarios.

Task 2: Identification of Potential Human Failure Events and Associated Unsafe Actions

This task is performed in two stages. The first is to identify the potential human failure events (HFEs).

Identification of Human Failure Events

The selection of individual HFEs is based on the system or functional requirements associated with the events associated with the event tree branch points. The HFEs will correspond to human caused failures at the function, system or component level, and at this stage are defined entirely in terms of failure modes. (Note that, as discussed in Reference 5, the events that are finally incorporated in the PRA model may be defined more precisely as arising from specific unsafe actions and specific reasons.) Since the failure modes in terms of their impact on the system are similar to those caused by hardware faults, they are limited in number.

For example, for the initiating event "loss of main feedwater" in a PWR, the preferred method of decay heat removal is generally identified as the use of the auxiliary feedwater system. The auxiliary feedwater system is a standby system for which the success criterion in this scenario is, for example, that one out of three pumps start automatically and that the system continue to provide water to the steam generators for 24 hours following loss of main feedwater. The analysis should consider the following HFEs as causes of failure of the auxiliary feedwater system. They are identified as resulting from errors of commission (EOC) or errors of omission (EOO)

to highlight the types of HFEs that are not normally included in PRAs.

Auxiliary feedwater system (AFWS) required to start on demand:

AFW equipment removed from automatic control (EOC),
Automatic start of AFWS not backed up when required (EOO).

AFWS required to continue running:

Emergency operating procedures, (EOPs) require that manual control of the AFW system is established following initiation. The appropriate human failure events are:

AFW resources inappropriately diverted (EOC or EOO),
AFW resources inappropriately depleted (EOC or EOO),
Operating AFW equipment inappropriately terminated (EOC),
Operating AFW equipment inappropriately isolated (EOC),
Equipment operation results in under-feeding/filling (EOC or EOO).

The errors of commission have not generally been represented in existing PRA models. Typically, only errors of omission, such as failure to start the AFWS manually as a backup to the auto-initiation signal, or failure to make up to the CST to supplement the inventory, have been included. These new HFEs should be considered as new failure modes for the top event Auxiliary Feed Water System failure.

The Identification of Potential Unsafe Actions

The next step in the process is to identify the different ways in which the operators could produce the effect characterized by the failure mode identified above. This requires a detailed understanding of the systems and how they are operated. The Frame of Reference Manual will contain guidance on the generic types of unsafe actions that might occur. These can be specialized to the AFW system, by identifying those that are applicable to that particular system. This requires detailed knowledge of system design and operational characteristics. The following are examples of specific unsafe actions that could apply to the AFW system:

Errors of Commission

The HFE 'AFW equipment removed from automatic control', could result from the following:

Initiation signals bypassed or suppressed,
Automatic signals taken out of "armed" status by placing pump start switches to manual,
Motive and/or control power to the pumps removed or disabled,
Taken out of standby status (e.g., pumps in "pull-to-lock").

The HFE 'AFW resources inappropriately depleted', could result from:

CST inventory being depleted prior to equipment initiation,
AFW equipment not re-aligned to secondary source when CST depleted.

Errors of Omission:

The HFE 'Automatic start of AFWS not backed up when required', is already at the level of an unsafe action, and no further decomposition is needed.

Task 3: Identification of the Most Probable/Significant Causes of the Unsafe Actions (EFC)

The purpose of this task in the application process is the identification and prioritization of the EFCs that are associated with the unsafe actions. This is the critical task that makes ATHEANA different from all other HRA methods. Essentially what the task entails is the construction of models for the causes of the unsafe action in terms of failure modes of the activities identified in a model of information processing (see for example Reference 6), and the EFC elements associated with those activities. For example, one possible model may begin by exploring the initial problem as being a failure in situation assessment. This results in an incorrect situation model, which leads to an inappropriate response plan, which if carried out correctly results in the unsafe action. However, the model for the unsafe action must also take into account the failures of the operators to realize their situation model is incorrect and take corrective action. The opportunity for this to occur may be after the response has been executed and the operators are monitoring the plant to determine whether the effect of the actions they have taken are having the expected effect. The opportunity may, on the other hand, occur before the response execution has been completed, and could be

triggered by new information.

In accordance with the analysis criterion that the actions of interest are those in which the crew behave in a rational manner, it is assumed that the operators are responding in accordance with "rules", which could be formal, e.g., procedures, or informal, e.g., good practice. The method of analysis then considers the identification of the rule that, when inappropriately applied, results in the unsafe action, and identifying the reasons why that rule could have been invoked. A similar approach was adopted in Reference 7, but in that work, only the formal rules provided by the emergency operating procedures were investigated. Furthermore, the model of causes of unsafe actions adopted was crude compared with that developed for ATHEANA.

Building the models of causes of unsafe actions requires making use of several different types of information. It uses information that characterizes how errors can occur in the different stages of information processing, and the factors that influence the occurrence of errors. In addition, it is necessary to understand how information can be distorted by plant conditions and design features so that operators can become confused as to the interpretation of indications. Generic descriptions of the ways in which plant physics/behavior, the algorithms that are used in instruments/indications, and other plant conditions can create confusion will be presented in the Frame of Reference Manual.

In the following paragraphs, a systematic and efficient approach to identifying the EFCs is outlined, focusing on the failures caused by problems in situation assessment. The approach is presented as a number of steps. At a high level, the unsafe action is considered to have arisen because the operators have an incorrect situation assessment model and fail to update it in a timely manner.

The first step is to determine if there is a rational explanation of why the unsafe action could be committed. This is done by identifying rules that the operators might apply to justify their actions, and which could apply for the PRA scenario of interest.

Step 1: For Each Unsafe Action Examine the "Rules" that Would Lead to the Unsafe Action

This is the first of a set of screening steps, and it is justified by the requirement that the operators' actions be rational. The purpose of this step is to identify reasons why the unsafe action would be performed, in terms of formal or informal rules of operation. So for example, for the unsafe action "SI inappropriately secured", the following types of rules might apply:

Formal

Procedure ES 0.1, Step x, SI Termination Criteria

Informal

The informal rules relate to behavioral responses that are ingrained as a result of training, such as:

Avoid going solid in the pressurizer,
Stop spurious SI,
Protect pump when you get a trouble alarm.

The next step is to determine what information the operators would use to apply the rules, and where the information would come from, and is essentially an information gathering step.

Step 2: Identify Information Needed to Use the Rules

This step should identify both the primary and secondary sources of plant information that might be used, and the standard practices that are adopted, e.g., look at ammeters as well as pump indicators. This can be regarded as establishing the operational practice that apply. Examples of the information needed to determine whether the conditions for applying the rule for SI termination are satisfied are:

Formal Rule (as identified above):

Pressurizer pressure
Pressurizer level
Subcooling margin
Secondary heat sink
- AFW flow
- Steam generator level

Informal rule:

Pressurizer level (if pressurizer solid rule)
Pressurizer level and pressure (if spurious SI rule)

The next step is to identify the ways in which the criteria in the rules could have been interpreted as having been met, even though they have in fact not been met. Essentially this requires that the information that is available has to have been distorted, either by plant

conditions, or by operator bias, or indeed both.

Step 3: Determine how the Rules Could Appear to Have Been Met When They in Fact Have Not Been

This step identifies the ways in which the incorrect situation model could have arisen, and also how information retrieval problems, plant conditions and physics problems, and operator problems (e.g., wrong mental model) could distort the information that should be seen by the operators.

However, in accordance with the PRA defined unsafe action, the incorrect situation model has to exist and persist until the unsafe action has manifested itself as a failure. This is addressed in the next step.

Step 4: Determine how the Operators Could Fail to Recognize that the Situation Model is Incorrect, and Correct it to Prevent Incorrect Application of Rule

This step is associated with the potential for recovery, and is needed to address the dynamic nature of response. This consists of a consideration of all stages of information processing. In this case, however, when the operators have initiated a response, the monitoring of the plant response, to confirm the appropriateness of the response that has been implemented is a key element for analysis.

Step 5: Identify the Potentially Significant Error-Forcing Contexts

This step corresponds to summarizing and analyzing the information obtained in the previous four steps. A key point here is to search for the EFC elements that both cause the initial error and inhibit the possibility of recovery. Selecting the potentially most significant depends on several factors, which are plant-specific, and will require the input of plant experts. That the EFCs are expected to contain several elements is illustrated by the EFC identified for the following real event.

Crystal River 3 stuck-open pressurizer spray valve:

In this event the unsafe action was an inappropriate termination of High Pressure Injection, and the following EFC elements contributed:

- pressurizer spray valve position indication was inconsistent with actual valve position (due to pre-existing hardware failure and design);
- no direct indication was available of pressurizer spray flow;
- evolution in progress was to increase reactor power (basis for the erroneous conjecture that under-power event occurred).

Task 4: Refinement of HFE Definitions and Integration into PRA Logic Model

The issues associated with the refinement of HFE definitions are discussed in Reference 5 and are not reproduced here. This is primarily a systems analysis function to address the potential for dependencies. The Implementation Guidelines will give guidance on how to account for dependency given the identification of the most significant EFCs associated with the unsafe actions and HFEs.

Task 5: Estimate the Likelihoods of the Error-Forcing Contexts and the Consequential Probabilities of the Unsafe Actions

The approach to quantification is to first estimate the likelihood of the EFCs associated with each unsafe action, and for each EFC, to estimate the conditional probability of error.

- The estimation of likelihoods of EFCs will be based on constructing probabilistic models for the joint occurrence of the elements of the EFC. This entails obtaining estimates of the relative frequency with which the conditions in the EFC occur in the PRA scenario definition That this is feasible has been demonstrated by the trial application in NUREG/CR-6350[3].

- Estimation of conditional probabilities of error given an EFC. This will be a function of how specific the EFC definitions will be. In the case that the EFC is defined such that failure is almost guaranteed, then there is no need to estimate this conditional probability. However, in many cases, the EFC creates an environment in which the likelihood of failure is enhanced, and in this case, it will be necessary to develop methods for estimating these probabilities.

Once the HFEs to be included in the PRA model have been defined and incorporated into the logic structure in the appropriate way, the requantification of the PRA model is essentially trivial.

IV SUMMARY

This paper has presented an overview of the ATHEANA method for HRA. The analytical process for application has been described, and the relationship to the two major documents that are in development, namely the Frame of Reference Manual and the Implementation Guidelines, has been discussed.

ACKNOWLEDGEMENTS

This work has been performed for the USNRC under a contract to Brookhaven National Laboratory. However, the opinions expressed in this paper are solely those of the authors, and do not necessarily represent those of the USNRC or BNL. The authors are grateful to Emilie Roth of the Westinghouse Corporation for significant technical input related to modeling of cognition.

REFERENCES

1. Barriere, M.T., W.J. Luckas, Jr., J. Wreathall, S.E. Cooper, D.C. Bley, and A. Ramey-Smith, *"Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis,"* NUREG/CR-6265, BNL-NUREG-52431, August 1995.

2. Barriere, M.T., Luckas, W.J., Whitehead, D.W., and Ramey-Smith, A., *An Analysis of Operational Experience During LP&S and A Plan for Addressing Human Reliability Assessment Issues*, NUREG/CR-6093, Brookhaven National Laboratory: Upton, NY and Sandia National Laboratories: Albuquerque, NM, 1994.

3. Cooper, S.E., Ramey-Smith, A., Wreathall, J., Parry, G.W., Bley, D.E., Taylor, J.H., and Luckas, W.J., *A Technique for Human Error Analysis (ATHEANA) - Technical Basis and Methodology Description*, DRAFT NUREG/CR-6350, to be published.

4. Cooper, S.E. et al, *Knowledge-Base for the New Human Reliability Analysis Method, "A Technique for Human Error Analysis" (ATHEANA),* in these proceedings

5. Parry, G.W., Luckas, W.J., Wreathall, J., Cooper, S.E., and Bley, D.C., *Process Description for ATHEANA: A Technique for Human Error Analysis*, Brookhaven National Laboratory Technical Report, L-2415/95-2, December 30, 1995.

6. Roth, E.M., Mumaw, R.J., and Lewis, P.M., *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*, NUREG/CR-6208, Westinghouse Science and Technology Center: Pittsburgh, PA, July 1994.

7. Julius, J.A., Jorgenson, E.M., Parry, G.W., and Mosleh, A.M., "A Procedure for the Analysis of Errors of Commission in a Probabilistic Safety Assessment of a Nuclear Power Plant at Full Power" *Reliability Engineering and System Safety*, Vol. 50, (1995), pages 189-201.

Figure 1

Process Flow Diagram