Philosophy of ATHEANA*

Dennis C. Bley
The WreathWood Group
bley@compuserve.com

Susan E. Cooper
SAIC
secemk@bellatlantic.net

John A. Forester
Sandia National Laboratories
JaFores@sandia.gov

Alan M. Kolaczkowski
SAIC
alan.m.kolaczkowdki@cpmx.saic.com

Ann Ramey-Smith
USNRC
ars@nrc.gov

Catherine M. Thompson
USNRC
cmt1@nrc.gov

Donnie W. Whitehead
Sandia National Laboratories
dwwhite@sandia.gov

John Wreathall
The WreathWood Group
jwreatha@columbus.rr.com

Abstract

ATHEANA, a second-generation Human Reliability Analysis (HRA) method, integrates advances in psychology with engineering, human factors, and Probabilistic Risk Analysis (PRA) disciplines to provide an HRA quantification process and PRA modeling interface that can accommodate and represent human performance in real nuclear power plant events. The method uses the characteristics of serious accidents identified through retrospective analysis of serious operational events to set priorities in a search process for significant human failure events, unsafe acts, and error-forcing context (unfavorable plant conditions combined with negative performance-shaping factors). ATHEANA has been tested in a demonstration project at an operating pressurized water reactor.

1. Introduction

This paper introduces a new, second-generation Human Reliability Analysis (HRA) method called "A Technique for Human Event Analysis," (ATHEANA). ATHEANA is the result of development efforts sponsored by the Probabilistic Risk Analysis Branch in the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission. ATHEANA has been developed to address limitations identified in current HRA approaches by:

- addressing errors of commission and dependencies,
- representing more realistically the human–system interactions that have played important roles in accident response, and
- integrating advances in psychology with engineering, human factors, and Probabilistic Risk Analysis (PRA) disciplines.

The ATHEANA technical basis and implementation guidelines are documented in a draft report that describes the basis for the method and the analysis process [1]. It provides step-by-step guidance on how to:

- select and organize the ATHEANA team,
- perform and control the structured search processes for human failure events and unsafe acts, along with the reasons that such events occur; i.e., the elements of error-forcing context (EFC),
- use the knowledge encoded in the PRA along with the specialized knowledge and experience of the team to focus the searches on those events and reasons that are most likely to affect the risk, and
- quantify the error-forcing contexts and the probability of each unsafe act, given its context.

*This work was supported by the U. S. Nuclear Regulatory Commission and was performed at Sandia National Laboratories. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the U.S. Department of Energy under Contract DE-AC04-94AL85000.

It is anticipated that practitioners of ATHEANA will be most concerned with the step-by-step guidelines. However, the team must include members who are thoroughly familiar with the knowledge base of theoretical material and operational events that underlie ATHEANA. Therefore, the report also summarizes the technical bases of ATHEANA. Theoretical material from the behavioral sciences explains the factors involved in human error. Application of theoretical models to real nuclear power plant events clarifies which factors are most often involved in significant events. Together, these expositions lead to formalisms for retrospective analysis of events and prospective analysis of human reliability. The report includes an appendix that describes a demonstration of ATHEANA at an operating nuclear power plant, the first test trial of ATHEANA (beyond the development group).

2. Background

The record of significant incidents in nuclear power plant operations shows a substantially different picture of human performance than that represented by human failure events modeled in PRAs. The latter typically represent failures to perform required procedure steps. In contrast, human performance problems identified in real operational events often involve operators performing actions that are not required for accident response and, in fact, worsen the plant's condition (i.e., errors of commission). Further, accounts of the role of operators in serious accidents, such as those that occurred at Chernobyl 4 [2,3] and Three Mile Island 2 (TMI-2) [4], frequently leave the impression that the operator's actions were illogical and incredible. Consequently, the lessons learned from such events often are perceived as being very plant-specific or event-specific.

As a result of the TMI-2 event, numerous modifications and backfits were implemented by all nuclear power plants in the United States, including symptom-based procedures, new training, and new hardware. After the considerable expense and effort to implement these modifications and backfits, the kinds of problems which occurred in this accident would be expected to be "fixed." However, there is increasing evidence that there may be a persistent and generic human performance problem that was revealed by TMI-2 (and Chernobyl) but not "fixed": errors of commission involving the intentional operator bypass of engineered safety features (ESF). In the TMI-2 event, operators inappropriately terminated high-pressure injection, resulting in reactor core undercooling and eventual fuel damage. NRC's Office of Analysis & Evaluation of Operation Data (AEOD) published a report in 1995 entitled "Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features"[5], identifying 14 events over the previous 41 months in which ESF was inappropriately bypassed. The AEOD report concluded that these events, and other similar events, show that this type of "... human intervention may be an important failure mode." Events analyses performed to support the ATHEANA project [1,6,7] have also identified errors of commission resulting in the inappropriate bypass of ESF.

In addition, event analyses of power plant accidents and incidents, performed for this project, show that real operational events typically involve a combination of complicating factors that are not addressed in current PRAs. Examples of such complicating factors in operators' response to events are:

- multiple (especially dependent or human-caused) equipment failures and unavailabilities,
- instrumentation problems, and
- plant conditions not covered by procedures.

Unfortunately, the fact that real events involve such complicating factors frequently is interpreted only as an indication of plant-specific operational problems, rather than a general cause for concern.

3. Underlying Principles of ATHEANA

The purpose of the ATHEANA development effort is to develop an HRA quantification process and PRA modeling interface that can accommodate and represent human performance found in real nuclear power plant events.

Based on observations of serious events in the operating history of the commercial nuclear power industry as well as experience in other technologically complex industries, the underlying basis of ATHEANA is that significant unsafe acts by humans occur as a result of combinations of influences associated with the plant conditions and specific human-centered factors that trigger errors by plant personnel. Error mechanisms are often not inherently bad; rather, they include some mechanisms that usually allow humans to perform skilled and speedy operations. For example, people often diagnose the cause of an occurrence based on pattern matching. Thus, physicians diagnose illnesses using templates of expected symptoms to which patients' symptoms are matched. This pattern-matching process is a way to make decisions quickly and usually reliably. If physicians had to revert to first principles to diagnose each patient, treatment would be delayed, patients would suffer, and the number of patients who could be treated in a given time would be severely limited. However, when applied in a certain specific context, such processing mechanisms can lead to inappropriate actions that can have

unsafe consequences. Continuing the medical analogy, the patterns of symptoms for diseases that are well understood in Western countries may not be so reliable if applied blindly in tropical third-world countries.

Given this perspective on the causes of human error, what is needed for the development of an improved HRA method is a process to identify the likely opportunities for inappropriately triggered mechanisms to cause errors and unsafe consequences. The starting point for this search is a multidisciplinary framework that seeks to describe the interrelationships among error mechanisms, the plant conditions and performance-shaping factors that set them up, and the consequences of the errors in terms of how the plant can be rendered less safe. The framework includes elements from the plant operations and engineering perspective, the PRA perspective, the human factors engineering perspective, and the behavioral sciences perspective. All of these contribute to our understanding of human reliability and its associated influences, and have emerged from a review of significant operational events at nuclear power plants by a multidisciplinary project team representing all of these disciplines. The elements included in the multidisciplinary framework are the minimum set necessary to describe the causes and contributions of human errors in a technological setting, for example, major nuclear power plant events.

The human performance-related elements of the framework are performance-shaping factors, plant conditions, and error mechanisms. These elements are representative of the understanding needed to describe the underlying causes of unsafe actions and hence explain why a person may perform an unsafe action. The elements relating to the PRA perspective, namely, the human failure events and the scenario definition, represent the PRA model itself. The unsafe action and human failure event elements represent the point of integration between the HRA and PRA model. The PRA traditionally focuses on the consequences of the unsafe action, which it describes as a human error that is represented by a human failure event. The human failure event is included in the PRA model associated with a particular plant state that defines the specific accident scenarios that the PRA model represents.

The framework has served as the basis for retrospective analysis of real operating event histories [1,6,7,8,9]. That retrospective analysis has identified the context in which severe events can occur; specifically, the plant conditions, significant performance-shaping factors (PSF), and dependencies that "set up" operators for failure. Serious events seem to always involve both unexpected plant conditions and unfavorable PSFs (e.g., situational factors) that comprise an error-forcing context. The term "plant condition" means both the physical condition of the nuclear power plant and its instruments. For example, the plant physical condition, as interpreted by the instruments (which may or may not be functioning as expected), is fed to the plant display system. Then the operators receive information from the display system and interpret that information (i.e., make a situation assessment) using their mental model and current situation model. The operator and display system form the human–machine interface (HMI).

Based on the operating events analyzed, the error-forcing context typically involves an unanalyzed plant condition that is beyond normal operator training and procedure-related PSFs. This error-forcing condition can activate a human error mechanism related to, for example, inappropriate situation assessment (i.e., a misdiagnosis), which can lead to the refusal to believe or recognize evidence that runs counter to the initial misdiagnosis. Subsequently, mistakes (e.g., errors of commission), and ultimately, an accident with catastrophic consequences can result. These ideas lead to another way to frame the observations of serious events that have been reviewed:

- the plant behavior is outside the expected range;
- the plant's behavior is not understood;
- indications of the actual plant state and behavior are not recognized; and
- prepared plans or procedures are not applicable or helpful.

From this point of view, it is clear that key factors in these events have not been within the scope of existing PRAs/HRAs. If these are the characteristics of severe accidents that actually occur, then expansion of PRAs/HRAs to model them is essential. Otherwise PRAs may not include the dominant contributors to risk.

Previous HRA methods have implicitly focused on addressing the question, "What is the chance of random operator error (e.g., operator fails to...) under nominal accident conditions?" Even when performance-shaping factors are included, they are typically evaluated for the nominal event sequence or, at best, for particular cut sets. The analyses have not looked beyond the hardware modeled in the PRA for specific conditions that could complicate operator response. Based on review of the operating experience in several industries, a more appropriate question to pursue is: "What is the chance of occurrence of an error-forcing context such that operator error is very likely?"

The ATHEANA method is based on a series of very simple premises:

- when required to respond to abnormal conditions in nuclear power plants, the operators' actions are based logically on their understanding of the conditions in the plant;

- the operators' understanding of conditions in the plant is produced by the evidence presented to them through the human–machine interfaces, their awareness of plant activities, and their knowledge of the behavior of plant systems;
- the operators' understanding of the state of the plant can be misled by combinations of plant conditions and weaknesses in the human–machine interface or gaps in job aids like the training and procedures under those plant conditions;
- the operators' misunderstanding of the plant state can lead them to take inappropriate actions, which can include actions to terminate operating equipment;
- this can involve a series of actions under dependent conditioning, despite a series of cues that otherwise could not be missed.

Identifying and assessing the likelihood of these inappropriate actions are the primary goals of the ATHEANA method.

The underlying steps for the ATHEANA method are summarized as follows:

- identify event sequences during which operators may inappropriately disable operating safety equipment or fail to actuate necessary equipment (i.e., the types of unsafe acts of interest) and thereby create potentially important contributions to plant risks of core damage or containment failure;
- identify the combinations of plant conditions and weaknesses in the human–machine interface or gaps in job aids that could mislead the operators into acting inappropriately on operating safety equipment under those plant conditions;
- estimate the likelihood of these combinations of plant conditions and weaknesses
- estimate the likelihood of operators performing the unsafe acts of interest under those conditions; and
- incorporate the effects of these inappropriate operator actions into the plant's PRA logic models and quantification process.

4. Error-Forcing Context

Work in the behavioral sciences has contributed to the understanding of the interactive nature of human errors and plant behavior that characterize the accidents that have occurred. This understanding suggests that it is essential to analyze both the human-centered factors (with consideration of such performance-shaping factors as human–machine interface design, procedures content and format, and training), and the conditions of the plant that give rise to the need for actions and create the operational causes (such as misleading indications, equipment unavailabilities, and other unusual configurations or operational circumstances). This is in contrast to the existing HRA methods that consider principally the human-centered causes, with only an acknowledgment of plant influences through such simplistic measures as "time available for action."

The human-centered factors and the influence of plant conditions are not independent of each other. Rather, major accidents create the need for operator actions under particular ("unusual") plant conditions in which mismatches between those "unusual" plant conditions and human-centered factors lead to unsafe acts on the part of people responding to the unusual plant conditions.

Therefore, typical evaluations performed in HRA assessments of performance-shaping factors, such as the layout indicators or control switches, may not identify critical problems unless the whole range of possible plant conditions under which the controls or indicators may be required is considered. In other words, a particular layout of indicators and controls may be perfectly adequate for the nominal conditions assumed for a PRA scenario. However, it is possible that there are other conditions that could arise during the same PRA scenario that could have an influence on the occurrence of operator errors in the accident response. For example, under the nominal conditions of an accident scenario, an operator may be required to perform a series of actions at locations on several control boards. Provided the actions can be well separated in time, the layout may prove adequate. However, it is possible that under some subset of plant conditions for the same scenario, the dynamics of the plant require the actions to be taken almost simultaneously. In this case, the layout is inadequate and might result in failure to perform the actions in time

Simply stated, operator failure in a PRA scenario is perhaps as likely, or more likely, to result from "off-normal" plant conditions during the scenario as it is to result from a random "human error" during the nominal conditions. Analyses of power-plant accidents and near-misses indicate that the influence of off-normal plant conditions appears to dominate over "random" human errors.

This evidence from incident analyses is consistent with experience described by training personnel who have observed that operators can be "made to fail" in simulator exercises by creating appropriate combinations of plant conditions and operator mindset. Examples of difficulties in operator performance in challenging simulator-training situations have been demonstrated by Roth et al. [10].

Unless the analysis of PSFs recognizes that plant conditions can vary significantly within the definition of a

single scenario in the current PRA, and that some of those plant conditions can be much more demanding of operators (both in terms of the plant conditions themselves and the limitations in PSFs such as procedures and training under those conditions), the analysis may fail to identify the most risk-significant conditions leading to operator failure.

Therefore, if it is to provide an effective tool for measuring and managing risk, PRA must be able to incorporate realistically both those human failure events that are caused by off-normal plant conditions and those that occur "randomly" during nominal accident conditions. However, for a PRA to incorporate unsafe acts caused by off-normal plant conditions, it is necessary to be able to estimate how likely these conditions are and the likely consequences in terms of inappropriate human actions or inactions.

The identification of these error-forcing contexts must be based on an understanding of the kinds of psychological mechanisms causing human errors that can be "set up" by particular plant conditions that lie within the PRA definitions of accident scenarios. Without such an understanding, the search for these error-forcing contexts would be limited to searches for "repeat events" that were simply duplicates of earlier incidents where people had failed, regardless of the frequency of or severity of consequence. It is important to find the more general class of events represented by these particular instances, if fixes are to be effective. For example, if an incident occurs and a human error is attributed to a deficient procedure, a particular fix may be to change that procedure to remove the immediate and direct cause of the error. Fixing the broader class would involve analyzing why the procedure was deficient. Was there an insufficient review? Were the conditions under which the procedure was to be used not described fully or accurately? What programmatic changes could remove not only that one particular flaw but other similar but undiscovered flaws in that and other procedures?

In other words, for an HRA to yield a practical set of tools, it must guide user-analysts in the search for conditions under which risk-important human errors are likely to occur and it must do this in an efficient and effective way.

5. The Process of ATHEANA

To support the PRA/HRA process, ATHEANA must transform the framework-based process for retrospective event analysis into a prospective process for identifying and quantifying unsafe acts and error-forcing context. That process must address several specific areas based on insights from the analysis of operating events and review of existing HRA methods.

5.1 Search Scheme for Human Failure Events (HFEs)

A search scheme is needed, especially for errors of commission and dependencies not previously identified in PRAs, but also for the more commonly modeled errors of omission because results to date have not been consistent across PRAs [11]. Most existing HRA methods allow the HFEs to fall naturally out of the review of emergency operating procedures, primarily by asking the question: "Do the operators carry out the actions that their procedures demand?" Severe, seemingly inexplicable errors, such as turning off operating safety systems, bypassing start signals, and defeating interlocks, are not generally modeled. However, such errors have occurred, and often for the best of reasons given operators' beliefs concerning the state of the plant and its likely response. The search for HFEs that is detailed in draft ATHEANA documentation begins as a PRA or systems-related search. It is a structured top-down approach. The first step in the search process is to use the PRA model to identify those functional failure modes that could be caused by rational human behavior.

The definitions of HFEs may initially be given at a very high level. For example, "Operator fails Safety Injection." However, more specific human failure events can be identified by linking HFEs with specific equipment failure modes. For example, "Operator fails ESFAS" can be decomposed into the unsafe acts "Operator bypasses ESFAS" and "Operator terminates ESFAS early." In principle, such decompositions can be determined a priori since the failure modes for equipment are the same whether from human or other causes.

An emphasis on comprehensiveness can be fatal if the level of effort is to be controlled and if the best thinking is to be directed to the most important problems. The search process defined in draft ATHEANA documentation proposes a way to narrow the scope of the HRA by focusing on highest priority issues first.

5.2 Search for Error-Forcing Context

Although a few existing methods flag the importance of context, none provides a practical search scheme for identifying and quantifying the error-forcing contexts. Because of the importance now attached to error-forcing context, this point alone means that a new method is required. That perception of importance is based on the simple observation that every serious event in the operating histories analyzed involves an error-forcing context as a function of the mismatch between plant

conditions and human-related conditions. The search for EFCs is a questioning process based on insights from the retrospective study of operating events that is intended to walk the analyst through a range of possible reasons (e.g., error mechanisms, PSFs, dependent effects, plant conditions). The structure for this questioning process and the tools for applying the process (i.e., structured tables of information) are summarized below.

In setting priorities and quantifying the probabilities of the HFEs, whether they are defined at a high level or at the level of an unsafe act, the HRA analyst will need to identify the potentially different EFCs that can result in a specific unsafe act. For example, "operator terminates ESFAS early" can occur for a variety of different reasons that can be logically explained and described by the combination of error mechanisms and error-forcing contexts.

The approach for identifying EFCs is based on two complementary perspectives: (1) an understanding of error mechanisms and their causes, to identify under what conditions people may be expected to fail and how plant-specific activities and systems could give rise to error mechanisms; and (2) plant engineering and operations, to identify particular activities and systems of the plant where vulnerabilities may result in core damage.

It is possible to think of the search for HFEs of the previous section as a human-centered failure modes and effects analysis (FMEA). Parallel to that characterization of the search for HFEs, the search process for the error-forcing context can be characterized as a human-centered hazard and operability (HAZOP) analysis [12]. The entire search process is formalized into a set of questions that an analyst can use as the basis for a systematic identification of HFEs, unsafe acts, and EFCs that is based on the theoretical concepts and experience that has been described earlier. This technique of asking a series of questions to structure the search is quite similar to the HAZOP approach developed in the chemical process industry. The HAZOP uses a multidisciplinary team to examine every aspect of a plant's design by asking questions based on a set of "guide words" that are established to test every conceivable deviation from design intent. In the new HRA approach, error mechanisms have been used to develop tools to help identify the factors that should define the EFCs of concern.

5.3 Quantification

In this new formulation, quantification becomes a question of evaluating how likely specific EFCs are within the wide range of alternative conditions. The chance of error given the EFC is evaluated by judgment tempered by available evidence, including the knowledge and experience of plant operators and trainers. Details are provided in the ATHEANA guidelines document [1].

6. Future Work

ATHEANA enters the realm of becoming a better-defined method with the publication of the technical basis and guidelines document [1]. Its basis is multidisciplinary, as is the problem it analyzes. That basis is expected to grow as more events are analyzed and as new work becomes available from the underlying disciplines. Therefore, refinements can be expected in the tools that support the process. However, the basic structure of the process should remain intact.

In the short term, three efforts are already under way:

- The ATHEANA guidance document is being revised and refined based on lessons learned from the application and peer review,
- ATHEANA will be used to investigate fire risk at a nuclear power plant, and
- The database of significant operating events is being expanded.

These tasks, in turn, will lead to additional refinements in ATHEANA.

In addition, the developers would like to see considerations associated with organizational factors integrated into ATHEANA.

Finally, it is recognized that many aspects of ATHEANA could be enhanced by the development of an automated user support system. The search process, which itself is being refined, may become less burdensome and more consistent if it is guided by an interactive computer program that could query and guide the user. The ability to link the search process for EFC with the database of real event histories would place the search for reasons on an example-based footing.

7. References

[1] *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)*, Draft report for comment, NUREG-1624, U.S. Nuclear Regulatory Commission, Washington, DC, April 1998.

[2] *Report on the Accident at the Chernobyl Nuclear Power Station*, NUREG-1250, U.S. Nuclear Regulatory Commission, Washington, DC, December 1987.

[3] *Implications of the Accident at Chernobyl for Safety Regulation of Commercial Nuclear Power Plants in the United States*, Vols. 1 and 2, Final Report, NUREG-1251, U.S. Nuclear Regulatory Commission, Washington, DC, April 1989.

[4] Rogovin, M., and G. Frampton, *Three Mile Island - A Report to the Commissioners and to the Public*, Special Inquiry Group, U.S. Nuclear Regulatory Commission, Washington, DC, January 1980.

[5] *Engineering Evaluation - Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features*, AEOD/E95-01, Office of Analysis and Evaluation of Operational Data (AEOD), U.S. Nuclear Regulatory Commission, Washington, DC, July 1995.

[6] Barriere, M.T., W.J. Luckas, J. Wreathall, S.E. Cooper, D.C. Bley, and A.M. Ramey-Smith, *Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis*, NUREG/CR-6265, Brookhaven National Laboratory Upton, NY, August 1995.

[7] Cooper, S.E., W.B. Luckas, and J. Wreathall, *Human-System Event Classification Scheme (HSECS) Database Description*, BNL Technical Report No. L2415/95-1, Brookhaven National Laboratory, Upton, NY, December 1995.

[8] Barriere, M.T., W.B. Luckas, D.W. Whitehead, and A.M. Ramey-Smith, *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, June 1994.

[9] Cooper, S.E., A. Ramey-Smith, J. Wreathall, G.W. Parry, D.C. Bley, J.H. Taylor, and W.J. Luckas, *A Technique for Human Error Analysis (ATHEANA)*, NUREG/CR-6350, Brookhaven National Laboratory, Upton, NY, April 1996.

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

[11] *Individual Plant Examination Program: Perspectives on Reactor Safety and Plant Performance*, Volumes 1 and 2, NUREG-1560, Division of Systems Technology - Office of Nuclear Regulatory Research, US Nuclear Regulatory Commission, Washington, D.C., October 1996.

[12] Knowlton, R.E., *An Introduction to Hazard and Operability Studies: The Guide Word Approach*, Chemetics International, 1992.