ATHEANA: A Technique for Human Error Analysis: An Overview of Its Methodological Basis

John Wreathall, The WreathWood Group, Dublin, Ohio
Ann Ramey-Smith, U.S. Nuclear Regulatory Commission, Washington, D.C.

Abstract

The U.S. NRC has developed a new human reliability analysis (HRA) method, called A Technique for Human Event Analysis (ATHEANA), to provide a way of modeling the so-called "errors of commission" - that is, situations in which operators terminate or disable engineered safety features (ESFs) or similar equipment during accident conditions, thereby putting the plant at an increased risk of core damage. In its reviews of operational events, NRC has found that these errors of commission occur with a relatively high frequency (as high as 2 or 3 per year) [3], but are noticeably missing from the scope of most current probabilistic risk assessments (PRAs). This new method was developed through a formalized approach that describes what can occur when operators behave rationally but have inadequate knowledge or poor judgement. In particular, the method is based on models of decisionmaking and response planning that have been used extensively in the aviation field, and on the analysis of major accidents in both the nuclear and non-nuclear fields. Other papers at this conference present summaries of these event analyses in both the nuclear and non-nuclear fields.

This paper presents an overview of ATHEANA and summarizes how the method (1) structures the analysis of operationally significant events, and (2) helps HRA analysts identify and model potentially risk-significant errors of commission in plant PRAS.

1. INTRODUCTION

The record of significant incidents in nuclear power plant (NPP) operations shows a substantially different picture of human performance than that represented by human failure events modeled in most typical probabilistic risk assessments (PRAs). The latter typically represent failures to perform required steps of a procedure. In contrast, human performance problems identified in real operational events often involve operators performing actions that are not required for accident response and that, in fact, worsen the plant's condition (i.e., errors of commission). In addition, accounts of the role of operators in serious accidents, such as the accidents that occurred at Chernobyl 4 [1] and Three Mile Island Unit 2 (TMI-2) [2], 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, there were numerous modifications and backfits 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 that occurred in the accident at TMI-2 would be expected to

be "fixed." However, there is increasing evidence that there may be a persistent and generic human performance problem which was revealed by TMI-2 (and Chernobyl) but not fixed: errors of commission involving the intentional operator bypass of engineered safety features (ESFs). In the TMI-2 event, operators inappropriately terminated high-pressure injection, resulting in reactor core undercooling and eventual fuel damage. NRC's Office for Analysis and Evaluation of Operational Data (AEOD) published a report in 1995 entitled "Operating Events With Inappropriate Bypass or Defeat of Engineered Safety Features" [3] that identified 14 events over the preceeding 41 months in which ESFs were 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 analyzed to support the ATHEANA project [4] also have identified several errors of commission resulting in the inappropriate bypassing of ESFs.

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 (1) multiple (especially dependent or human-caused) equipment failures and unavailabilities,(2) instrumentation problems, and (3) 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 as a general cause for concern.

The purpose of ATHEANA is to develop a human reliability analysis (HRA) quantification process to support PRA to accommodate and represent human performance found in real NPP events.

Observations of serious events in the operating history of the commercial nuclear power industry and experience in other technologically complex industries indicate that the underlying basis of ATHEANA: significant human errors occur as a result of combinations of influences associated with the plant conditions and specific human-centered factors that trigger error mechanisms in the plant personnel. These error mechanisms are often not inherently bad behaviors but are usually mechanisms that allow humans to perform skilled and speedy operations. For example, people often diagnose the cause of an occurrence by the technique of pattern matching. Physicians diagnose illnesses by using templates of expected symptoms to which patients' symptoms are matched. This pattern-matching process enables physicians to make decisions quickly and usually reliably. If physicians had to revert to first principles with 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 the wrong context, these mechanisms can lead to inappropriate actions that can have unsafe consequences.

Given this basis for 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 that can have unsafe consequences. The starting point for this search is a framework that seeks to describe the interrelationships between error mechanisms, the plant conditions and performance shaping factors that set them up, and the consequences of the error mechanisms in terms of how the plant can be rendered less safe.

The framework is discussed at length in Reference 4. It contains elements from the plant operations and engineering perspective, the PRA perspective, the human factors engineering perspective, and the behavioral sciences perspective - all of which contribute to our understanding of human reliability and its associated influences. It was developed from the review of significant operational events at NPPs by a multidisciplinary project team representing all of these disciplines. Its elements are the minimum necessary set to describe the causes and contributions of human errors in, for example, major NPP events.

The human performance-related elements of the framework (i.e., those requiring the expertise of the human factors, behavioral science, and plant engineering disciplines) 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 models. 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, which 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 [4, 5, 6]. That retrospective analysis has identified the context in which severe events can occur; specifically, the plant conditions, significant performance shaping factors (PSFs), and dependencies that set operators up for failure. Serious events seem to always involve both unexpected plant conditions and unfavorable PSFs (e.g., situational factors) that constitute an "error-forcing" context. To clarify the term "error-forcing" context, we mean those conditions whereby an unsafe action becomes significantly more likely than compared with other conditions that may be nominally similar in terms of a PRA-based description (for example, a small loss-of-coolant accident with failure of high-pressure injection to operate).

Plant conditions include the physical condition of the NPP and its instruments. The plant condition, as interpreted by the instruments (that may or may not be functioning as expected), is fed to the plant display system. Finally, the operators receive information from the display system and interpret that information (i.e., assess the situation) using their mental model and current situation model. The operator and display system form the human-machine interface (HMI).

The operating events analyzed indicate that the error-forcing context typically represents an unanalyzed plant condition that is beyond normal operator training and procedure-related PSFs. For example, this error-forcing condition can activate a human error mechanism related to 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. Consequently, mistakes (i.e., errors of commission) and, ultimately, an accident with catastrophic consequences can result.

2. BASIC PRINCIPLES OF ATHEANA

There have been many attempts over the past 30 years to gain a better understanding of the causes of human error. The main conclusion from the ATHEANA project is that few human errors represent random events; instead, most can be explained on the basis of how people process information in complex and demanding situations. Therefore, it is important to understand the basic cognitive processes associated with plant monitoring, decisionmaking, and control, and how these can lead to human error. The main purpose of this section is to describe the relevant models in the behavioral sciences, the mechanisms leading to failures, and the contributing elements of error-forcing contexts in power-plant operations. The discussion is based largely on the work of Dr. Emilie Roth, whose assistance is acknowledged here.

The basic model underlying the work described in this section is an information processing model that describes the range of human activities required to respond to abnormal or emergency conditions. The major cognitive activities represented in this model are (1) situation assessment, (2) response planning, (3) response implementation, and (4) monitoring and detection.

Situation Assessment: When confronted with indications of an abnormal occurrence, people actively try to construct a coherent, logical explanation to account for their observations; this process is referred to as situation assessment. Situation assessment involves developing and updating a mental representation of the factors known, or hypothesized, to be affecting plant state at a given point in time. The mental representation resulting from situation assessment is referred to as a situation model. The situation model is the person's understanding of the specific current situation, and it is constantly updated as new information is received.

Situation assessment is similar in meaning to "diagnosis" but is broader in scope. Diagnosis typically refers to searching for the cause(s) of abnormal symptoms. Situation assessment encompasses explanations that are generated to account for normal as well as abnormal conditions. Situation models are constantly updated as the situation changes. In power-plant applications, maintaining and updating a situation model entails keeping track of the changing factors influencing plant processes, including receipt of plant information, and results in an understanding of faults, other operator actions, and automatic system responses.

Situation models are used to form expectations, which include the events that should be happening at the same time, how events should evolve over time, and effects that may occur in the future. People use expectations in several ways. Expectations are used to search for evidence to confirm the current situation model. People also use expectations they have generated to explain observed symptoms. If a new symptom is observed that is consistent with their expectations, they have a ready explanation for the finding, giving them greater confidence in their situation model.

When a new symptom is inconsistent with expectations, it may be discounted or misinterpreted so as to make it consistent with the expectations derived from the current situation model. For example, on numerous occasions operators have failed to

detect key signals, or have detected them but misinterpreted or discounted them, because of an inappropriate understanding of the situation and the expectations derived from that understanding.

However, if the new symptom is recognized as an unexpected plant behavior, the need to revise the situation model will become apparent. In that case, the symptom may trigger situation assessment activity to search for a better explanation of the current observations. In turn, situation assessment may involve developing a hypothesis for what might be occurring, and then searching for confirmatory evidence in the environment. Thus, a situation assessment can result in the detection of abnormal plant behavior that might not otherwise have been observed, the detection of plant symptoms and alarms that may have otherwise been missed, and the identification of problems such as sensor failures or plant malfunctions.

The importance of situation models, and the expectations based on them, cannot be overemphasized. Situation models not only govern situation assessment, but also are important in guiding monitoring, in formulating response plans, and in implementing responses. For example, people use expectations generated from situation models to anticipate potential problems, and in generating and evaluating response plans.

Response Planning: Response planning refers to the process of making a decision about what actions to take. In general, response planning involves operators using their situation model of the current plant state to identify goals, generate alternative response plans, evaluate response plans, and select the most appropriate response plan relevant to the current situation model.

Although this is in the basic sequence of cognitive activities associated with response planning, one or more of these steps may be skipped or modified in a particular situation. For example, in many cases in NPPs, when written procedures are available and judged appropriate to the current situation, the need to create a response plan in real time may be largely eliminated. However, even when written procedures are available, some aspects of response planning will still be performed. For example, operators still need to (1) identify appropriate goals based on their own situation assessment, (2) select the appropriate procedure, (3) evaluate if the actions defined in the procedure are sufficient to achieve those goals, and (4) adapt the procedure to the situation if necessary.

Response Implementation: Response implementation refers to taking the specific control actions required to perform a task. It may involve taking discrete actions (e.g., flipping a switch) or it may involve continuous control activity (e.g., controlling steam generator level). It may be performed by a single person, or it may require communication and coordination among several individuals.

The results of actions are monitored through feedback loops. Two aspects of nuclear power plants can make response implementation difficult: time response and indirect observation. Plant processes cannot be directly observed; instead they are inferred through indications,

and thus, errors can occur in the inference process. The systems are also relatively slow to respond in comparison to other types of systems such as those in aircraft. Since time and feedback delays are disruptive to the execution of responses because they make it difficult to determine that control actions are having their intended effect, the operator's ability to predict future states using mental models can be more important in controlling responses than feedback.

In addition, response implementation is related to the cognitive task demands. When the response demands are incompatible with response requirements, operator performance can be impaired. For example, if the task requires continuous control over a plant component, then performance may be impaired when a discrete control device is provided. Such mismatches can increase the chance of errors being made. Another factor is the operator's familiarity with the activity. If a task is routine, it can be executed automatically, thus requiring little attention.

Monitoring and Detection: Monitoring and detection refer to the activities involved in extracting information from the environment. They are influenced by two fundamental factors: the characteristics of the environment and a person's knowledge and expectations. Monitoring that is driven by characteristics of the environment is often referred to as data-driven monitoring. Data-driven monitoring is affected by the form of the information - its physical salience (e.g., size, color, loudness). For example, alarm systems are basically automated monitors that are designed to influence data-driven monitoring by using aspects of physical salience to direct attention. Characteristics such as the auditory alert, flashing, and color coding are physical characteristics that enable operators to quickly identify an important new alarm. Data-driven monitoring is also influenced by the behavior of the information being monitored such as the bandwidth and rate of change of the information signal. For example, observers more frequently monitor a signal that is rapidly changing.

Monitoring can also be initiated by the operator on the basis of knowledge and expectations about the most valuable sources of information, typically referred to as knowledge-driven monitoring. Knowledge-driven monitoring can be viewed as active monitoring because the operator is not merely responding to characteristics of the environment that "shout out" like an alarm system does, but is deliberately directing attention to areas of the environment that are expected to provide specific information.

Knowledge-driven monitoring typically has two sources. First, purposeful monitoring is often guided by specific procedures or standard practice (e.g., control panel walkdowns that accompany shift turnovers). Second, knowledge-driven monitoring can be triggered by situation assessment or response planning activities and is, therefore, strongly influenced by a person's current situation model. The situation model allows the operator to direct attention and focus monitoring effectively. However, knowledge-driven monitoring can also lead operators to miss important information. For example, an incorrect situation model may lead an operator to focus his attention in the wrong place, to fail to observe a critical finding, or to misinterpret or discount an indication. This failure to detect discrepancies between what the operator expects and the actual plant conditions has been seen often in

accidents. It is a major factor in operators failing to recover abnormal situations for extended periods. For example, in an event at Oconee, Unit 3 [7], operators overlooked at least six cues, any one of which should have caused the operators to realize that they were not properly understanding what was wrong.

Typically, in power plants, an operator is faced with an information environment containing more variables than can realistically be monitored, Observations of operators under normal operating and emergency conditions make it clear that the real monitoring challenge comes from the fact that there are a large number of potentially relevant things to attend to at any point in time and that the operator must determine what information is worth pursuing within a constantly changing environment. In this situation, monitoring requires the operator to decide what to monitor and when to shift attention elsewhere. These decisions are strongly guided by an operator's current situation model. The operator's ability to develop and effectively use knowledge to guide monitoring relies on the ability to understand the current state of the process.

Under normal conditions, situations are assessed by mapping the information obtained in monitoring to elements in the situation model. For experienced operators, this comparison is relatively effortless and requires little attention. During unfamiliar conditions, however, the process is considerably more complex. The first step in realizing that the current plant conditions are not consistent with the situation model is to detect a discrepancy between the information pattern representing the current situation and the information pattern detected from monitoring activities. This process is facilitated by the alarm system that helps to direct the attention of a plant operator to an off-normal situation.

When determining whether or not a signal is significant and worth pursuing, operators examine the signal in the context of their current situation model. They form judgments with respect to whether the anomaly signals a real abnormality or an instrumentation failure. They will then assess the likely cause of the abnormality and evaluate the importance of the signal.

3. CONCLUSIONS

ATHEANA is currently under an initial trial application at a U. S. commercial NPP. This initial trial appears to indicate that the method can identify potentially significant human actions that are not in the spectrum of human actions normally represented in PRAs. The separate consideration of the four stages in the information-processing model appears to help identify different ways in which unsafe actions can come about. Work is continuing to develop the final details of the process used to quantify these failures.

4. REFERENCES

[1] P. P. Read, Ablaze: The Story of the Heroes and Victims of Chernobyl. New York:

Random House, 1993.

[2] J. Kemeny, The Need for Change: Report of the President's Commission on the Accident at Three Mile Island. New York: Pergamon Press, 1979.

[3] J. V. Kauffman, "Engineering Evaluation: Operating Events With Inappropriate Bypass or Defeat of Engineered Safety Features," report of the Office for Analysis and Evaluation of Operational Data, U.S. Nuclear Regulatory Commission, Washington, D.C., July 1995.

[4] M. T. Barriere, J. Wreathall, S. E. Cooper, D. C. Bley, W. J. Luckas, and A. Ramey-Smith, Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis, U.S. Nuclear Regulatory Commission, NUREG/CR-6265, August 1995.

[5] M. Barriere, W. Luckas, D. Whitehead, A. Ramey-Smith, D. C. Bley, M. Donovan, W. Brown, J. Forester, S. E. Cooper, P. Haas, J. Wreathall, and G. W. Parry. An Analysis of Operational Experience During Low Power and Shutdown and a Plan for Addressing Human Reliability Assessment Issues, U.S. Nuclear Regulatory Commission, NUREG/CR-6093, June 1994.

[6] S. E. Cooper, A. Ramey-Smith, J. Wreathall, G. W. Parry, D. C. Bley, W. J. Luckas, Jr., J. H. Taylor, and M. T. Barriere. A Technique for Human Error Analysis (ATHEANA), NUREG/CR-6350, May 1996.

[7] U. S. Nuclear Regulatory Commission, "Oconee Unit 3, March 8, 1991, Loss of Residual Heat Removal," U.S. Nuclear Regulatory Commission Report AIT 50-287/91-008, Washington, D.C., April 10, 1991.