ANS PSA 2011 International Topical Meeting on Probabilistic Safety Assesment and Analysis
Wilmington, NC, March 13-17, 2011, on CD-ROM, American Nuclear Society, LaGrange Park, IL (2008)

SAND2011-0469C

TOWARDS AN IMPROVED HRA QUANTIFICATION MODEL[1]

Gareth W Parry
ERIN Engineering and Research Inc.
2001 N. Main Street, Suite 510
Walnut Creek, CA, 94596, USA
gwparry@erineng.com

John A Forester, Katrina Groth, and Stacey M L Hendrickson
Sandia National Laboratories
PO Box 5800
Albuquerque, NM, 87185, USA
jafores@sandia.gov, kgroth@sandia.gov, smhendr@sandia.gov

Stuart Lewis
Electric Power Research Institute
942 Corridor Park Blvd, Knoxville, TN, 37932, USA
slewis@epri.com

Erasmia Lois
U.S. Nuclear Regulatory Commission
Washington DC, 20001, USA
Erasmia.lois@nrc.gov

ABSTRACT

The U.S. Nuclear Regulatory Commission and the Electric Power Research Institute are working together under a memorandum of understanding to improve the state of the art in human reliability analysis (HRA) by incorporating an understanding of the causes of human failures and the contextual factors that influence the likelihood of failures based on a review of relevant behavioral science and cognitive psychology literature. This paper outlines a decision-tree approach that is being developed for the estimation of human error probabilities (HEPs) that is consistent with that understanding.

Key Words: Human Reliability Analysis (HRA), Cognitive Mechanisms, Performance Influencing Factors (PIFs)

---

[1] The opinions expressed in this paper are those of the authors and not those of the USNRC or of the authors' organizations. Part of this work was funded by the U.S. Nuclear Regulatory Commission (USNRC) at Sandia National Laboratories (Sandia), a multi-program laboratory operated and managed by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

1 INTRODUCTION

The Nuclear Regulatory Commission's (NRC's) Office of Nuclear Regulatory Research (RES) is working with the Electric Power Research Institute (EPRI) under a Memorandum of Understanding to address the challenge presented in a Staff Requirements Memorandum (SRM) [1]. This SRM directed the NRC's Advisory Committee on Reactor Safeguards (ACRS) to "work with the staff and external stakeholders to evaluate the different human reliability models in an effort to propose a single model for the agency to use or guidance on which model(s) should be used in specific circumstances."

A significant part of the effort so far has been directed to developing an understanding of how failures of an operating crew to respond correctly to disturbances to the steady state operation of a plant can occur. This has resulted in the identification of a number of proximate causes of failure of each of a set of so-called macrocognitive functions, such as detection, sensemaking or understanding, decision-making, coordination or communication, and action, primarily at an individual level. For each of the proximate causes, one or more failure mechanisms have been identified based on a review of the relevant cognitive science and behavioral science literature. A failure mechanism is characterized by a cognitive mechanism or process and the specific situational or context factors that, when present, can result in failure to perform the required function. In this paper, the context factors are collectively referred to as performance influencing factors (PIFs) and include both aspects of the traditional performance shaping factors (PSFs) such as training, experience, man-machine interface, etc., and plant conditions that characterize the PRA scenario associated with the human failure event (HFE). In characterizing the failure mechanisms it is recognized that the PIFs are not independent but are interrelated as a function of the cognitive processes taking place. This information is being used as input to the development of guidance for the qualitative analysis that is required for an HRA, and, as discussed in this paper, for the development of an improved quantification model for the evaluation of the probabilities of the HFEs of the PRA model. Because the development work has not been completed, this paper focuses on one approach being pursued, and the characteristics of the approach.

The approach discussed here is a model based on identifying a set of mutually exclusive crew failure modes (CFM), and for each CFM, developing a decision tree. The contribution to the HEP for a specific HFE from each CFM is determined by the probability associated with the end point of the path through the tree that is determined by answering a series of questions related to the PIFs, designed to be as objective as possible, based on the PRA scenario-specific definitions of the HFEs, and on an understanding of the operational practices. The operational practices encompass such aspects as the procedures relevant to the scenario, training, and experience to establish those elements of context associated with each CFM as determined by the underlying cognitive mechanisms identified in the literature search discussed above. While these decision trees have a superficial resemblance to the decision trees of the cause based decision tree [CDBT] approach [2], the latter were developed in a somewhat intuitive way, whereas this new model is based on the understanding of cognitive failure mechanisms, and in so doing is consistent with the insights drawn from the psychological and behavioral science literature.

Section 2 discusses the issues associated with developing a quantification model and provides a brief description of the proposed approach. Section 3 provides discussion of the identification and definition of the CFMs. Because the final set of decision trees has not been finalized, the approach taken in Section 4 is to discuss in general terms and provide examples of the branch point structure and the questions that are used to assess the significance of the PIFs as a function of the context associated with a specific HFE.

2 FORMULATION OF THE QUANTIFICATION MODEL

An HFE defined in a PRA essentially defines a failure of the operating crew to correctly carry out a required response. The PRA scenario definition of the HFE includes identification of the information that is needed for the operators to make a correct situation assessment and the steps the operators need to take to get that information, what the procedure directs them to do, the time available to achieve success in the required response, and also the potential for additional cues and associated procedural guidance as the plant state changes. It also includes a specification of the plant state, i.e., which systems/components are operating, which are failed or unavailable (which is usually the reason for the required operator action), and, depending on the detail in the PRA model, may include information such as whether the required information is available. These conditions collectively define the boundary conditions for which the quantification model evaluates the HEP for the associated HFE.

In any interaction of the crew with the plant, there is a continuous interchange of information between the plant and the operating crew and between individual crew members that allows for "mid-course correction" of an initial error under the appropriate conditions. In other words, there are, in many cases, opportunities and sufficient time for recovery of an initial error; success in recovery would prevent the functional failure represented by the HFE from happening. The recovery potential will be different depending on the cause of failure of the initial error. The proposed approach discussed here is to incorporate the potential for recovery implicitly in the construction of the quantification model.

Because it is based on an understanding of the causes of human failures, the approach taken in this project is to develop a causal model of the failure, the causes being the ways in which the crew can fail the required function. While this could be developed to a very fine level of detail, modeling each individual crew member separately for example, this would rapidly become very complicated. The level of decomposition chosen is that of a set of causes for which the probabilities of their occurrence as a function of the scenario will be determined by the characteristics of the PIFs that are relevant to those causes. The causes are expressed in terms of the failures in the interface of the crew and the system, so that the causes are related to failures to get the right information, failures to adopt the correct response (given correct information), and failures in execution (given they are following the correct procedure). These are meaningful in the context of modeling the system as a whole (plant, procedures, MMI, crew), and are at the same level as the modeling of hardware. For example, PRAs typically model the ways in which a pump might fail (fails to start, fails to run) but don't model the different causes of the failure of a pump to start, although some of the "PIFs" that affect the pump failure probability (e.g., type of medium (dirty vs. clean), type of pump, etc.) may be used to identify different sub-populations of pumps with their own failure probabilities. While it is possible to model human failure causes at

a different level, e.g., failure in understanding, such a failure cause is very general and is not directly translatable to a consequence that is relevant to the system. It is a potential cause of several of the higher level failure causes above.

The approach is based on identifying a set of crew failure modes (CFMs). The CFMs represent ways in which the crew can fail to achieve the function. They are the explanations at a fairly high level of why the HFE occurs (e.g., crew dismisses relevant information that results in their failure to achieve the required response). They are causes at the system level, but not at the human level – they explain how the crew failed but not why. The HEP is calculated using the following equation:

$$HEP(HFE|S) = \sum_i Prob\ (\mathrm{CFM}_i|S)$$

where S is the PRA scenario that leads to the requirement for the operating crew response whose failure is characterized by the HFE. With this construct, the CFMs are considered to be mutually exclusive.

The quantification model for the probability of each CFM is based on the understanding of the required crew response, and on the understanding of the human failure mechanisms alluded to in the introduction above. For the CFMs to be the interface between the HFE and the PIFs, the HFE occurs as the result of the persistence of the CFM long enough to cause the plant to change state irreversibly, i.e., mid-course correction has not been successful. As mentioned in the introduction, the approach described in this paper is to adopt a decision tree format, with a probability associated with each path through the tree.

A decision tree (DT) is to be constructed for each CFM. Each DT is given a title that represents the initial human failure. Each path through the decision tree represents a different explanation of why the HFE occurs, and includes consideration of failure to recover from the initial human error. The DTs are therefore an integral model of the HFE. The direction taken at each branch of each decision tree is determined by the answers to a set of questions that relate to the existence or not of critical PIFs. The concept behind this form of the quantification model is that it will prompt the analyst to assess the existence of and/or the "strength" or relevance of those factors that have been identified as affecting the occurrence and persistence of each CFM. The information concerning these factors is determined either directly from the definition of the PRA scenario S (typically plant conditions, procedural guidance, timing information), or needs to be determined by review of operating practices, details of the procedures, the nature of the training and experience, etc. (the more traditional PSFs).

The PIFs that are relevant to each CFM are based on the results of the literature survey to identify those factors (those embedded in the definition of S and the PSFs) that can result in the CFM together with an explanation (the psychological/behavioral model) of why they are relevant. The literature search started with observed human failures, and then searched for an explanation in terms of a cognitive model, and the PIFs that resulted in the failure modes. Thus it seems to be natural to associate the CFMs with the failure modes. A failure mode is, in the words of the ASME/ANS PRA standard, "a specific functional manifestation of a failure (i.e., the means by which an observer can determine that a failure has occurred) by precluding the successful operation of a piece of equipment, a component, or a system (e.g., fails to start, fails to run, leaks)".

This approach is, in many ways, similar to that of the MERMOS approach [3]. Each path through the decision tree represents what in MERMOS would be called a human failure scenario, and the CFMs correspond roughly to the CICAs.

3 IDENTIFICATION OF CREW FAILURE MODES

The set of CFMs is identified based on an understanding of the functions the crew needs to perform in order to correctly carry out the required response. The crew can be considered to fail because at some level it:

- Fails to achieve a correct situation assessment, and therefore, fails to understand the plant status and the nature of the upset
- Fails to choose the correct response strategy given a correct situation assessment
- Fails to execute the response strategy correctly

The aim is to develop a set of CFMs that are relevant to the NPP PRA context. In the NPP control room context the crew is operating with a well defined human-system interface (HIS), and a set of procedures that provide guidance to the crew in their response to upset conditions. In order to achieve a correct situation assessment, the crew has to respond to the information from the plant (cues), and interpret that information correctly in terms of directing them to the appropriate procedure.

An initial set of CFMs is presented below. Note that these are preliminary and subject to change. The development of the decision trees may indicate duplication of causal descriptions. The reconciliation of the search for psychological mechanisms that lead to failure may also lead to new CFMs.

In addition to plant parameters, information can come in the form of alarms. Some alarms, such as reactor trip, are signals to enter the EOPs. Others lead to alarm response procedures. In some cases, the alarm is sufficient to identify the upset condition and give a clear situation assessment. In other cases, the procedure leads the operators through a set of diagnostic steps to identify the appropriate response (e.g., for a Westinghouse plant, the steps of E-0 provide a directed search for the relevant parameters to determine if E-1, E-2, or E-3 (or one of a number of other procedures) is the appropriate procedure to follow for the plant conditions). Alarms that require immediate response are treated differently from directed search for information (e.g., plant parameters) as a result of procedural direction.

Failures in Information Gathering and Interpretation – (Situation Assessment)

- Alarm not attended to [human causes include alarm dismissed as not being important]
- Required information not searched for [human causes include data not attended to and premature termination of search for relevant data]
- Information received too early and forgotten [could apply to a condition that is not immediately significant but could become so as the accident progression – e.g., a trouble alarm on a piece of equipment that is not needed immediately]

- Information not checked with appropriate frequency [e.g., incorrect sampling strategy - significant for monitoring activities]
- Information discounted/dismissed [would apply to an alarm or a piece of data that has been obtained as a result of direction]
- Data misperceived [human causes include miscommunication between crew members]
- Wrong data attended to

Note that there is no implication that the concern should be with a single piece of information. However, the implication is that the information of concern is needed for the correct situation assessment. For example, there are some cases where several pieces of data are required to be checked (e.g., for terminating SI), others where it is simpler and only one piece is required. In addition, some data is the primary data, and other data is confirmatory. Confirmatory data would be most likely interpreted as providing a potential for recovery.

Failures in Decision given Success in Situation Assessment:

- Misinterpret procedures [this is more likely to be a concern when the logic in the procedures is somewhat convoluted]
- Defer action [this is applicable mainly to procedural directions that are not written as requiring immediate execution]
- Choose inappropriate strategy including deciding to use the wrong system [should apply only when there are alternate viable strategies – when using EOPs one human cause could result from the crew attempting to recover a primary system rather than employing a strategy that would prevent core damage but could potentially be economically harmful to the plant (e.g., using bleed and feed)]
- Deviate from procedures [should only be considered in a PRA if the procedures do not apply]

Failures in Execution (Action) given Success in Situation Assessment and in Choosing an Appropriate Response Strategy:

- Don't complete action ["Don't complete action" may be decomposed into skip a step; failure to start action; and take too long/delay)
- Commit wrong action ["Commit wrong action" may be decomposed into mis-execute the action; use the wrong system/equipment)
- Reversal of actions where sequencing matters.

Note that all these CFMs may be inferred from the crew responses without having to delve into the reasons why they might occur. The mechanisms for these CFMs are captured in the construction of the decision trees.

4 CONSTRUCTING THE DECISION TREES

The paths through the decision trees represent the set of human failure scenarios considered to be representative for the nuclear power plant context. Each path identifies the PIFs

that enable a particular cognitive mechanism to lead to a response that if uncorrected would lead to failure, and also identifies the factors that make that failure persist long enough to actually result in failure. The branches are chosen to represent a decision on the existence of factors included in the definition of the human failure scenarios based on an understanding of the human failure mechanisms identified as discussed above, and on the nature of, and the general characteristics of the operating crew approach to performing, the tasks required. These factors include aspects of the scenario characteristics, e.g., complexity of signature, ambiguity of signature, conflicting tasks (workload), crew expectations (resulting in bias, too early an SA etc.) influenced by training and experience, aspects of teamwork, and potential for recovery.

The determination of whether a factor is applicable for a specific HFE is made by responding to a number of questions that are constructed to be as objective as possible, to reduce the inter-analyst variability prevalent in current HRAs. These questions will provide guidance on the qualitative analysis that has to be performed to support the HRA for the determination of the PIFs. As an example, one of the factors considered in a human failure scenario could be the role of confirmatory data in providing a means of recovery. To determine whether such a recovery is possible, the questions will need to elicit such things as whether the crew routinely searches for confirmatory data, whether the data is easy to get, etc. The point is that the analysts will need to build a qualitative picture of the data collection process employed by the crew and make an assessment of which is crucial, and which is not, and answer the relevant questions associated with the DTs in that light.

The CFM, Inappropriate Sampling Strategy, is discussed here to illustrate further the approach to developing the decision trees. This CFM applies to cases where the cue for taking an action is that a critical plant parameter (or parameters) has been reached. This failure mode represents the situation where the crew has recognized that the data is required to take an action, but they do not check it frequently enough so that when the critical value is reached, it is not recognized. Based on the survey of the literature, two possible failure mechanisms were identified. The first is a mismatch of the crew's expectations when compared with the specific situation for which the HFE is being evaluated, e.g., the crew expects that the rate of change of the critical parameters to be much slower than they actually are. The second is that there are other activities that are equally or more pressing and provide a distraction from the information gathering. While the second could exist on its own, it could also be a complicating factor for the first failure mechanism.

The following PIFs were identified as being relevant to the occurrence of these failure mechanisms.

- Training. The specific issue related to training is whether it provides the crew with strong expectations of how quickly the critical parameter values change. While this expectation may be appropriate for most scenarios, there may be circumstances where the rate of change of parameter values is slower or more rapid than the scenarios for which they have been trained. Thus, the task for the analyst is to determine whether these circumstances exist for the specific HFE being considered.
- Loads. The issue of concern is whether there are coincident tasks requiring attention. If there are, the questions that need to be answered include: whether these other demands are determined to be more urgent, whether they are alternate approaches to

dealing with the upset condition, and whether the resources required to complete the conflicting tasks put a serious constraint on the task of interest.

- System Responses. How fast do the parameters change?
- Teamwork. How is the work coordinated, and how is the task load distributed?

In constructing the decision tree, the following candidates for the branch points are discussed together with examples of the types of questions that are associated with the branch points. While the branch points are numbered, there is no implication that this will necessarily be the order in which they would appear on the decision tree.

BP 1: Are there coincident tasks?

The purpose of this branch point is to identify whether, for the PRA scenario being considered, there is an equally (or more) pressing response related to a different safety function that is required. The concern is that this would increase workload and increase the chance of failing to monitor effectively by providing a distraction. Whether this condition exists can be answered Yes or No directly from an understanding of the accident sequence being considered.

BP2: Are there other success paths that would be routinely tried first to achieve success in the same function?

Again, the concern here is whether there is a potential for distraction, exacerbated by the desire not to use the ultimate success strategy, which would usually provide more of a challenge to the restart of the plant. The existence of alternate success paths can be determined directly from an understanding of the procedures, training and operating practices as they relate to the task whose failure is modeled in the HFE.

BP3: Is there a mismatch with crew expectations regarding the rate and nature of the change of the parameter?

To answer this as yes or no would require answering several subsidiary questions. The questions will be constructed in a hierarchical manner so that they lead to an unambiguous choice. So, for example, they could include:

Is this scenario, or one close to it, addressed in training so that the crew is able to formulate an expectation? If this type of scenario is not addressed in training, the YES branch would be taken.

If the type of scenario is addressed in training, the following questions would be asked:

What does the crew training lead them to expect with respect to the rate of change of the parameter being monitored?

Is the expectation compatible with the rate of change for this specific scenario? If the response is positive, the NO branch would be taken. If the response is negative, the following question would be asked:

Is the rate of change is faster or slower than the expected? The significance of the expectation would be followed up in the assessment of the monitoring strategy.

BP4: Is the monitoring strategy optimized for success?

Whether or not there are coincident activities that are being attended to, the issue of concern is whether the parameter is considered important enough to give it adequate attention. Questions that may be asked include:

Is there a particular crew member whose task it is to monitor this parameter? The answer to this would be expected to be in the affirmative.

Will the parameter be monitored continuously or intermittently?

If it is monitored intermittently, is there a common practice for the frequency of checking the value?

If the frequency of monitoring can be determined, is it adequate to detect the critical change?

BP5: Is there an alarm associated with the critical value of the parameter?

The existence of the alarm would provide a powerful recovery mechanism for this particular CFM. Whether the YES or NO branch is taken would relate to the effectiveness of the alarm. This might differ depending on the path through the tree. For those paths for which there are coincident tasks of alternate success strategies, it might be easier for the crew not to pay attention to the alarm, or to recognize its relevance. Questions concerning this alarm would include:

Is the response required to the alarm clearly understood, as a result of training for example?

Is its meaning unambiguous?

Are the operators trained to respond to the alarm regardless of what else is going on?

Thus the quantification model will consist of a number of decision trees, one for each CFM. Each decision tree consists of the branching structure supported by a set of questions, the answers to which determine which path is taken at each branch. A probability will be determined for each individual path based on an expert elicitation process. The experts will assess these probabilities based on a consideration of the complete human failure scenario as a means of taking into account the dependence between the PIFs. While the approach has not yet been finalized, one suggestion that appears to have some merit is to rank the probabilities of the paths through the tree for each tree separately, assess the probabilities associated with an optimal and the least optimal path, and by a process of interpolation, establish the probabilities of the intermediate scenarios.

5. SUMMARY

The approach outlined in this paper for the quantification model for HRA is one approach to improving the consistency and reproducibility of the derivation of HEPs for well-defined HFEs. The approach is based on an understanding of human failure mechanisms consistent with current theories and practices in the behavioral science and cognitive psychology disciplines.

6 REFERENCES

1. US Nuclear Regulatory Commission, *Staff Requirements—Meeting with Advisory Committee on Reactor Safeguards, SRM M061020*, US Nuclear Regulatory Commission, November 8, 2006, Washington, DC.
2. *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment*. June, 1992. EPRI TR-100259.
3. P. Le Bot, et al. "MERMOS, a Second Generation HRA Method: What It Does and Doesn't Do", *Proceedings of the American Nuclear Society International Topical Meeting on Probabilistic Safety Assessment (PSA '99)*. American Nuclear Society, August 1999.