SANDIA REPORT
SAND2008-5085
Unlimited Release
Printed January 2009

An Overview of the Evolution of Human Reliability Analysis in the Context of Probabilistic Risk Assessment

John A. Forester, Susan E. Cooper, Alan M. Kolaczkowski, Dennis C. Bley,
John Wreathall, and Erasmia Lois

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

NOTICE: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof, or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government, any agency thereof, or any of their contractors.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2008-5085
Unlimited Release
Printed January 2009

An Overview of the Evolution of Human Reliability Analysis In the Context of Probabilistic Risk Assessment

John A. Forester
Risk & Reliability Analysis Department
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-0748

Susan E. Cooper and Erasmia Lois
U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Washington, DC 20555

Alan M. Kolaczkowski
Science Applications International Corporation
1342 Manzana St.
Eugene, OR 97404

Dennis C. Bley
Buttonwood Consulting Inc.
11738 English Mill Ct.
Oakton, VA 22124-2253

John Wreathall
John Wreathall and Co.
4157 MacDuff Way
Dublin, OH 43016

Abstract

Since the Reactor Safety Study in the early 1970's, human reliability analysis (HRA) has been evolving towards a better ability to account for the factors and conditions that can lead humans to take unsafe actions and thereby provide better estimates of the likelihood of human error for probabilistic risk assessments (PRAs). The purpose of this paper is to provide an overview of recent reviews of operational events and advances in the behavioral sciences that have impacted the evolution of HRA methods and contributed to improvements. The paper discusses the importance of human errors in complex human-technical systems, examines why humans contribute to accidents and unsafe conditions, and discusses how lessons learned over the years have changed the perspective and approach for modeling human behavior in PRAs of complicated domains such as nuclear power plants. It is argued that it has become increasingly more important to understand and model the more cognitive aspects of human performance and to address the broader range of factors that have been shown to influence human performance in complex domains. The paper concludes by addressing the current ability of HRA to adequately predict human failure events and their likelihood.

Acknowledgments

This work was funded by the U.S. Nuclear Regulatory Commission and performed at Sandia National Laboratories. Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000. The opinions expressed in this paper are those of the authors and not of the U.S. Nuclear Regulatory Commission.

Table of Contents

Table of Tables

Table of Figures

1. ARE HUMAN ERRORS IMPORTANT IN COMPLEX HUMAN-TECHNICAL SYSTEMS?

Three Mile Island (TMI), Chernobyl, Bhopal, Challenger, Air Florida Flight 737, Piper Alpha – these names are etched in our consciousness. All were accidents where safe and trusted technologies went awry. All involved extensive property damage and most were serious disasters with many deaths. One brought no death or injury, but substantial emotional trauma to workers and nearby population. The technologies involved were hardly related, even for the two nuclear plant accidents. All were designed to high-reliability standards, generally incorporating redundancy (multiple identical components), diversity (functional redundancy), and extensive training for operators and maintenance personnel. What went wrong? Were these simply random events, bad rolls of the dice? Or is there a common thread among them?

Figure 1. Chernobyl and TMI - Common Elements in Very Different Accidents.

Following the 1986 accident at Chernobyl in the Ukraine, the view in the west was summed up by the UKAEA report *The Chernobyl Accident and Its Consequences* [1], "It seems certain that a Chernobyl-type accident could not happen in the UK...the Chernobyl accident was unique to the RBMK reactor design and there are few lessons for the United Kingdom to learn from it. Its main effect has been to reinforce and reiterate the importance and validity of existing UK safety standards." Indeed it was clear that the Chernobyl design was unforgiving and there was a strong view that plant operators felt free to experiment with their reactor.

However, from another point of view, a re-framing if you will, one can see disturbing similarities to the very different sequence of events at Three Mile Island (TMI) some years earlier. Beginning with Chernobyl, we can identify three crucial stages of the accident that strongly affected human performance: Plant personnel placed the reactor in an unusual and unanalyzed condition (the emergency core cooling system was disconnected and power was reduced for a diesel generator test leading to rules on power and reactivity being violated for an extended time)

- Operators did not understand the core physics in this unusual condition
- Operators and managers refused to believe instrument readings and field reports, because of their incorrect understanding

At TMI, a remarkably similar series of human conditions played out:

- A "work-around" (using instrument air to unblock resin beds) caused a reactor trip; and unexplained maintenance tagout (disabling) of the emergency feed water supply starved cooling water to the steam generators; and a relief valve failure (sticking open) combined with a lack of understanding of the actuation signal for valve position indication led to an unrecognized condition in the reactor
- Operators did not understand the reactor physics in this unusual condition

Operators refused to believe implications of what they assumed were incorrect instrument readings

Those of us in the west had good reason to look on Chernobyl as a unique design problem; a physically similar accident couldn't happen with U.S. light water reactors. However, when we re-frame the very different physical accident at TMI, we find striking similarities. In both cases, the reactors were driven into modes of operation not familiar to the operators. Not understanding the physical regime, psychological traps kept the operators from acting appropriately on the cues coming to them from the plant. In both cases, operators took actions that seemed reasonable from their mistaken understanding of plant conditions that made the situation much worse (see comparison in Figure 1).

The 1982 Air Florida Flight 737 crash into the 14th Street Bridge in Washington, D.C. [2] was widely publicized. On departure from Washington National Airport, the plane accelerated slowly. The First Officer warned of an instrument/throttle anomaly, but was over-ruled by the pilot and the plane crashed into the 14th Street Bridge and Potomac River. There were only five survivors. The Pilot and First Officer were concerned about weather but failed to abide by relevant rules and take needed and possible actions to counter the post-takeoff performance problem. There were serious equipment problems: ice and snow caused reduced lift and increased drag and ice on the inlet pressure probe caused an erroneously high thrust indication, but experienced pilots were able to counter these problems in re-enactment simulations.

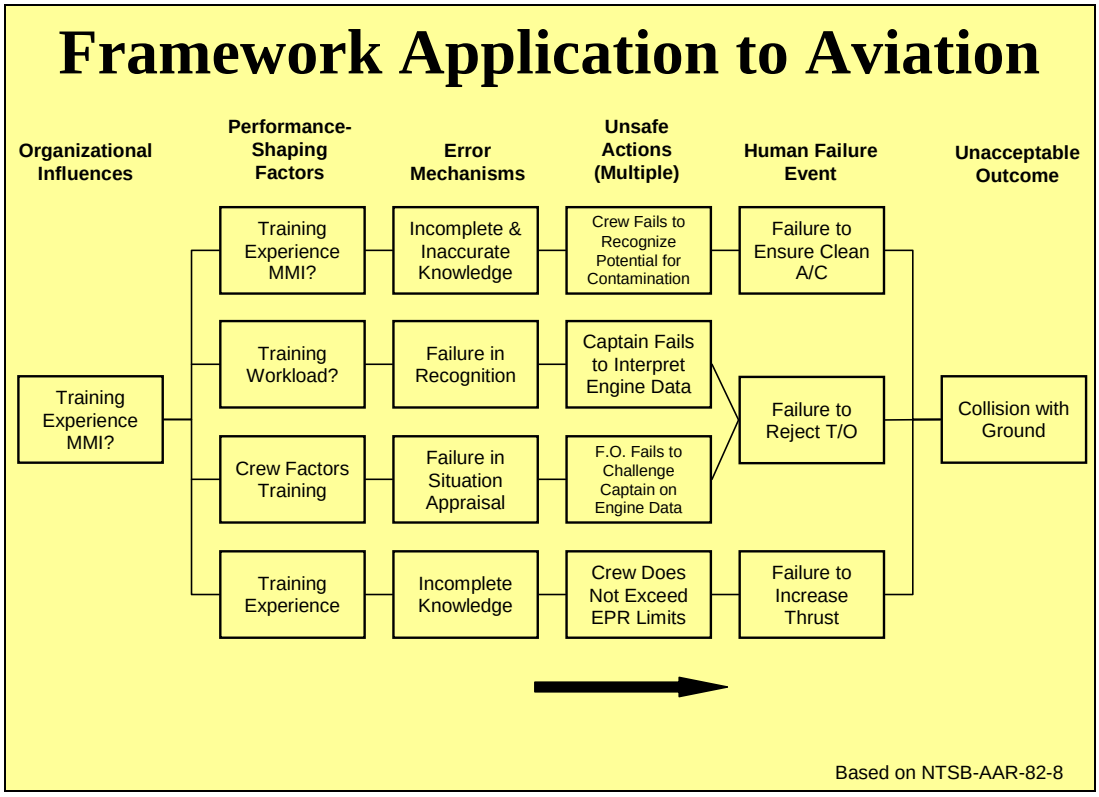


Figure 2. Framework Application to Aviation.

An analysis of the National Transportation Safety Board (NTSB) report [2] on the Air Florida crash is presented in Figure 2. Here we see the events of January 18, 1982 laid out against the ATHEANA (A Technique for Human Event Analysis) framework (NUREG-1624, Rev. 1, [3]) described later in this paper. It begins by showing that the "Organizational Influences" relevant to the accident had direct impact on four performance shaping factors (PSFs). The report emphasized that the training and experience of the crew were weak in ensuring an understanding of the situation and did not ensure that the best use of the knowledge of all crew members was involved in operational decisions. Four trains of influence lead to three

specific human failure events that all contributed to the collision. They each begin with PSFs that lead to human error mechanisms that lead to unsafe actions. The unsafe actions were influenced by four contingent conditions (akin to plant conditions in nuclear power plant operations):

- Weather conditions - perfect for icing
- Inadequate deicing solution
- Delay between deicing and takeoff
- B-737 aircraft pitch-up conditions

Crew training and experience led to an incomplete and inaccurate knowledge of icing conditions and the effects of contamination from exhaust gases. Thus, they failed to recognize the potential for contamination and ice build up on their aircraft caused by their actions. In addition, crew training and workload led to a failure to recognize relevant information, which in turn meant that the captain did not grasp the meaning of anomalous engine data. Finally, crew organizational training led to an error mechanism of failing to develop an adequate situation appraisal, which led the first officer to fail to sufficiently challenge the captain on the meaning of the engine data. Together these unsafe acts formed the human failure event: captain fails to reject takeoff.

Even though the captain went ahead with the takeoff, it should still have been possible to overcome the difficulties and successfully gain altitude. However, another aspect of training led to the captain's incomplete knowledge of the situation. He refused to exceed aircraft stress limits, because he did not understand the seriousness of the situation. An increase in thrust was the only chance he had to avoid the accident, which he failed to do.

This analysis of the accident can be summarized in findings similar to those for TMI and Chernobyl:

- Crew circumvented the rules – they did not verify the plane free of snow and ice; they used reversed thrust to melt it (which actually makes this condition worse); they failed to use engine anti-ice

- They were operating the plane in a regime they did not understand - this Florida crew had limited experience with the effects of special conditions on ice formation on the aircraft

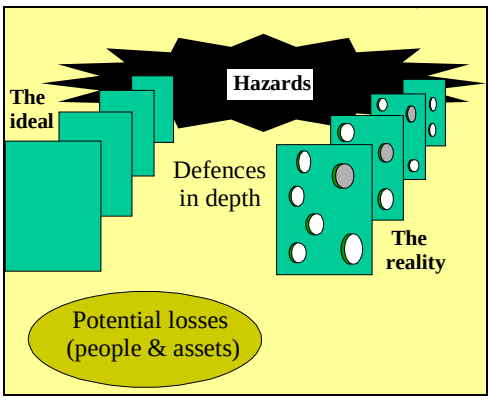
- The pilot refused to believe the evidence – instrument anomalies pointed out by the First Officer were ignored or overlooked

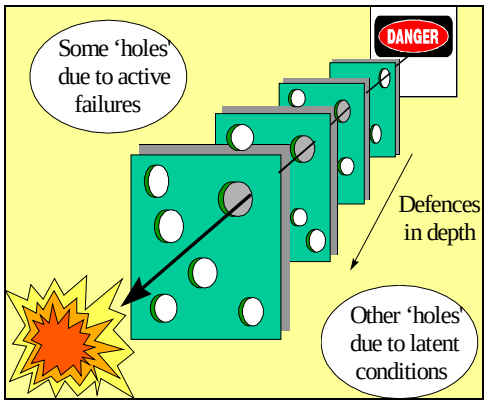
Once again we see an event where a combination of abnormal operating conditions and human conditions combined to set the operators up for failure. Analyses of other well known events have led to similar findings. The explosion at the Bhopal, India insecticide plant that killed at least 2,500 people and injured more than 200,000, the crash of the Challenger space shuttle, and the Piper Alpha oil platform explosion, all involved significant human actions

affected by similar characteristics.

Looking beyond these high profile events, statistics related to the occurrence of accidents in complex human technical systems suggest that the human contribution is relatively high. For example, as reported by Reason [4] and Hollnagel [5], data from the nuclear power industry [6, 7] indicated that 51% of 180 "significant" events in 1983 and 1984 could be attributed to human performance problems of some kind. Hollnagel [5] points out that the fraction is really higher because many of the other events examined in the Institute of Nuclear Power Operations (INPO) studies were related to design deficiencies and poorly manufactured equipment, which also could be attributed to human actions. The pattern seems to be generally the same in other industries. For example, Gertman and Blackman [8] and Hollnagel [5] reported that, regardless of the domain, there seemed to be general agreement that 60-90% of all system failures could be attributed to erroneous human actions.

Many of the accidents that have occurred in complex human-technical systems, involve "system" or hardware problems or other "environmental" factors, in addition to multiple human errors contributing to the accident. In fact, in many cases, serious events occur because of a combination of unusual conditions and latent human errors that trigger active human errors (Reason, [4]). Active errors are those that have an immediate effect on system performance and are usually made by system operators (e.g., pilots, train engineers, control room operators). Latent errors are those that do not have an immediate effect on system performance, but whose consequences can become important at a later time, particularly when something else goes wrong. Reason's [9] "Swiss Cheese" model (Figures 3 and 4) illustrates how latent errors generally have no impact on safe operation, but when the latent errors and hazardous plant conditions align in an unfortunate way, failure can result.





Figures 3 and 4. Illustration of Reason's [9] "Swiss Cheese" Model.

Latent errors are often related to maintenance tasks or may have been imbedded during the design phase. At TMI, personnel had tagged out and de-energized pumps that are normally in a standby condition. When cooling water was needed, the pumps were unavailable. In a related manner, the valve position indicator light circuit in the control room was designed such that it indicate open when the signal to open is sent rather than when the valve is actually

opened. This can also be classified as a latent error if operators normally assume that if the light indicates open, then the valve is open. Kletz [10] points out that instruments should measure the parameter that the operator wants to know. Measuring other parameters and calculating the desired information is possible, but often leads to misunderstanding and error.

The events described above illustrate situations where adverse system conditions and human errors had to occur in order for the accident to happen. The important point is that, although accident rates in complex human-technical systems are demonstrably low and efforts continue to keep them that way, serious accidents can and do occur and humans frequently contribute to their occurrence through inappropriate actions.

Those using and operating complex human-technical systems are very aware of the potential consequences of accidents in their domains and realize that safe operation requires appropriate actions on the part of operating crews and other personnel, whether under normal or accident conditions. To support personnel in their various capacities and to minimize the chances of inappropriate or unsafe human actions, most industries have instituted a significant number of safety-related conditions and controls. For example, the nuclear power industry has taken significant measures to minimize the chances of unsafe acts in nuclear power plants including:

- appropriate staffing levels,
- significant personnel education, frequent training, and updates on potential concerns and problems identified at other plants,
- procedures, plans, and checks to ensure that both maintenance during power operations and outage related activities are conducted safely,
- post-maintenance testing,
- symptom-based procedures for use in the control room,
- well-designed human-machine interfaces, including redundant and alternative instrumentation and related indications,
- industry initiated programs to improve human performance, and
- a strong emphasis on safety in performing one's job.

2. WHY DO HUMANS CONTRIBUTE TO ACCIDENTS AND UNSAFE CONDITIONS, IN SPITE OF COUNTERMEASURES?

A series of event investigations have revealed a common set of characteristics that consistently recur. In many instances they result from "mismatches" between some aspect of the system conditions and the human's expectations or understanding of the system. They tend to occur in combination and, except when the time available for successful response is extremely short, involve at least two contextual elements – both a complicating physical condition and a complicating human condition. With respect to the time limitation, some aircraft and train accidents are so unforgiving and fast that successful human response is not possible (i.e., time frames for responses are only on the order of seconds). Most light water nuclear power plants have substantial recovery capability, with time frames on the order of minutes to hours. The

following characteristics are usually identified in serious accidents:

- The system (plant, airplane, etc.) is in a deviant or unexpected state. System behavior and conditions are not usual or expected.

- System behavior and conditions are not understood by operators. Operators do not correctly identify the current and future system states, including the system's trajectory of states.

- Indications of actual system state and behavior are not recognized. Operators are provided with wrong or misleading information about the system state. Or, operators discount or reject helpful information.

- Prepared plans or procedures do not apply or are not helpful. Procedures, training, and other prepared plans do not address the actual system behavior and conditions.

- Informal rules are used that counter formal rules or plans. Operators inappropriately follow informal rules (e.g., "rules of thumb," informal training, informal interpretations of company policy or expectations, experience, folklore) that conflict with procedures, formal training, and/or other prepared plans.

- Breakdown in crew performance occurs. Crew performance is less successful than expected, either due to vulnerabilities in crew characteristics or due to specific features of the event context that defeat measures for improving crew performance.

An important point to be gleaned from these observations and the reviews of events is that there is usually a context associated with such accidents that contributes to the occurrence of unsafe acts. That is, serious accidents are not typically caused by random or un-forced errors on the part of negligent or inattentive operators. Rather, there are often several "sub-events" (e.g., hardware failures, environmental factors, unsafe design decisions, both latent and active human errors) that occur over time. And, it is the unique conjunction or concatenation of these events that leads to or essentially "sets up" the occurrence of the accident. In other words, the human error that most directly leads to the accident is often itself forced or driven by the context created by the sub-events.

One implication of these observations is that, in most cases, "human error" is somewhat of a misnomer. Operators in these situations usually are not just committing random errors or "making stupid mistakes," but rather they are taking actions that are reasonable given the information available, their understanding of the context, and their usual way of doing things. Dekker [11] provides a lively discussion of these issues and provides welcome guidance on how to evaluate events from the point of view of the operator involved in the action (i.e., a person "inside the tube" of the context who does not have the certain knowledge of how things will have turned out). In other words, from a global point of view, there are many aspects of the situation working against them with respect to making the correct decision and taking (or not taking) the

appropriate action. In hindsight, it may be possible to see where individuals made wrong choices and to argue that if they were any "good" they could have made better choices. But, expecting someone to "see through" the context at that particular moment in time may be very unrealistic.

This view considers most errors to be *consequences* rather than *causes* (Reason [4]) and is important because it leads analysts to investigate problems in the overall system that could arise and lead operators to take unsafe actions, rather than just blaming the human for failing to act appropriately. This position allows a broader and more realistic perspective on how to institute "fixes" in the system in order to help prevent humans from taking unsafe actions. Thus, in order to help move away from the tendency to focus on the "errors" made by humans when something goes wrong, the term unsafe actions[1] will be used instead of human error where appropriate in the rest of the article.

Besides the above mentioned unsafe actions, other more simplistic types of errors such as "slips" and "lapses of memory" do occur and can lead to serious consequences. That is, sometimes "inadvertent" errors do occur in which the person intends to take the correct action, but either takes a wrong action (a slip) or fails to take the action they intended (a lapse). Simple examples would include turning the wrong switch when the correct one is located next to it or inadvertently leaving out a step in a procedure when they fully intended to complete the step. Slips and lapses are often responsible for latent errors in maintenance, but are less frequently a problem where immediate feedback is available (e.g., in nuclear power plant control rooms, or in airplane cockpits, where such errors generally lead to an obvious change in system state). Of course, even these types of "errors" are frequently contributed to by outside causes (e.g., an individual is momentarily distracted) and will not always be "un-forced" errors on the part of the human.

Human reliability analysis (HRA), and particularly its use in nuclear power plant probabilistic risk assessment (PRA), is a formalized analytical technique for examining the potential for nuclear power plant operators to perform unsafe actions or inadvertent errors and, if appropriate, estimate the likelihood of these actions or errors. These techniques embody the use of task analysis, models, data, and judgment to assess operator performance and its impact on the overall risk from potential nuclear power plant accidents, including operator unsafe acts and errors that may contribute to those accidents. Before we describe both HRA and PRA in more detail, it is useful to discuss the discipline of behavioral science and how some of the knowledge from this discipline contributes to and forms many of the bases for how HRA is performed.

3. WHAT DO THE BEHAVIOR SCIENCES SAY ABOUT THE CAUSES OF UNSAFE ACTIONS?

[1]Unsafe actions are defined as actions taken, or not taken when needed, by operators or "plant" personnel that result in a degraded system safety condition. As described above, often they can only be called inappropriate in hind-sight.

Human reliability analysis (HRA), as mentioned above (and which will be discussed in more detail later), relies on knowledge from both the worlds of engineering and the behavioral sciences. The world of engineering describes the contexts and consequences of the unsafe actions. The world of the behavioral sciences describes the ways in which the contexts of the actions influence the likelihoods of different types of unsafe actions. The emphasis in this discussion is on human performance and unsafe actions in responding to abnormal occurrences– this is the most common type of action modeled in HRA. While this performance is typically associated with operators responding to abnormal events, it can also often apply to actions by maintenance crews performing work during routine conditions.

Of course, the world of the behavioral sciences encompasses much more than human performance in relation to the operation of technological systems. Models or theories exist from the very microscopic levels (e.g., the physiology of the central nervous system–the CNS), to the macroscopic studies of societies. While some aspect of these extremes of focus may play a role in understanding human performance related to nuclear power (e.g., the physiology of the CNS limits the speed with which people can recognize alarms, cultural aspects of society can influence the prioritization of responding to technical problems), the most relevant focus in the behavioral sciences is on the cognitive functions of operators (e.g., control room operators in power plants, pilots in aircraft, anesthesiologists in surgery). Cognition and, particularly, its subset of information processing, are a relatively new area of psychology that focuses on the mental processes, including detection, situation analysis, and problem solving. The earliest systematic work in this area was in the late 1950's to the middle 1960's. (See the discussions by Harré & Lamb [12] and Reason [4] for reviews of the development of the field).

Developments in the behavioral sciences have continued to expand the understanding of human performance issues required for PRA modeling. Firstly, work by Swain and Guttmann [13] set out many of the basics that underlie the early methods of human reliability analysis, with its emphasis on issues associated with such failures as selecting wrong instruments and controls, missing steps in procedures, and so on, that were seen as the critical issues in human performance before the accidents at Three Mile Island and Chernobyl. Following these accidents, work began on developing methods to model the likelihood of misunderstanding accidents as they evolve, such as the work discussed by Rasmussen & Rouse [14], Hall, et al. [15], Woods, et al. [16], and Dougherty & Fragola [17]. This work started to focus attention on the process of decision making by operators in the post-accident phase of nuclear plants. Particularly, the work by Woods and Roth (described in Woods, et al. [16]) and Reason [18], led to an upsurge in research to explain the issues associated with the identification and understanding of plant conditions. For example, Reason proposed a relatively straightforward model (GEMS) for the occurrence of unsafe actions that relies on the notion of schemas (e.g., Minsky [19]; Rumelhart [20]) and various human information processing and decision making heuristics (e.g., Tversky and Kahneman [21]). Following these developments, and continuing experience with human actions associated with misunderstandings by operators in responding to unusual plant conditions, developments took place to create newer HRA models that use as their basis a more complete understanding of the interactions between people and the systems. For example, later work by Woods et al. [22], Hollnagel [23, 24], Roth, et al. [25] and Reason [18]

all added significantly to the explanation of how people can be led to misunderstand the nature of events. This explanation underlies several of the more recent methods like ATHEANA [3] and CAHR (Sträter [26]; Sträter and Bubb [27]).

There are two fundamental models that are important in understanding the underlying methods of HRA and its role in PRA. The first is a representation of the substantially different kinds of failures that can occur. The second is the representation of information processing in humans (including small teams) associated with identifying and responding to substantial events.

3.1. Representation of Different Types of Failures - Slips and Lapses, Mistakes, and Violations

One of the most useful distinctions in the behavioral sciences about the nature and causes of unsafe actions is the breakdown between slips and lapses, mistakes, and violations (Norman [28]; Reason [4]). While this distinction post-dates some of the early HRA methods development, it provides a very useful way of distinguishing the different types of unsafe actions from a behavioral sciences perspective, and for which different HRA techniques are required. As discussed briefly above, *slips and lapses* are the erroneous actions that occur when people are following a planned set of actions and, because of a slip in attention or a lapse of memory (for example), the actions are not executed as intended. Examples in power plant operations include inadvertently selecting the wrong switch among a bank of similar switches, reading the wrong indicator for a plant parameter, or simply forgetting to turn a switch that they intended to turn (a lapse). Such errors become more frequent when a task follows a familiar routine up to a point, and then different actions from the normal task are called for. In this case, a slip or lapse will often occur when the person continues to follow the familiar routine that, in this instance, is wrong. An every-day example occurs when a person is driving along a familiar route to work, but on this day, intends to go to a different destination (perhaps the doctor's office). They suddenly 'wake up' and realize they have actually arrived in the parking lot at the work location – not where they had intended to arrive.

In contrast, *mistakes* are the class of errors that occur when a person is following a plan diligently, but the plan is inappropriate for the actual situation. The plan may be inappropriate because the person misunderstands the situation and persistently acts on their belief (as when the operators believed that the reactor system was going 'solid' at Three Mile Island and terminated high-pressure injection cooling as discussed in Kemeny [29]), or because the plan is inadequate and the person implementing it has insufficient knowledge to recognize the flaws. There are two subcategories of mistakes: rule-based and knowledge-based. Rule-based mistakes are associated with following 'rules,' typically those provided in procedures and standard operating practices in industrial settings, where either the wrong rule is being followed (as at Three Mile Island), or the rule is inadequate for the situation. Knowledge-based mistakes occur when a person is using their education and knowledge (rather than procedures and common learned practices) and that knowledge is incorrect or incomplete, or inaccessible in the stress of the moment.

Violations are different from the other two categories in that people knowingly and

deliberately break the rules, but without any intention of harm. Examples of violations would be the cases where a task requires a sequence of actions to be taken that involve moving from one location to another, back to the first location and then back to the second, and where the movement involves arduous or frustrating activities–for example, having to change into and out of radiation protective equipment. Suppose the people performing the task have learned from experience that in most cases, the actions at the distant location can be performed all at one time with no immediately noticeable adverse consequence. A likely violation would be that people routinely will perform the task using this short cut. Many times it may not matter, but when an occasion arises where the difference is important, a surprising failure will occur. (Often, the term "circumvention" is used for this type of error in the nuclear and other well-regulated industries because the term "violation" has a specific legal connotation, related to breaking laws and regulatory rules that are separate from human performance issues. However, for the purposes of this discussion we will keep the term "violation," as used by Reason and others in the behavioral sciences.)

This classification of errors is related to a second taxonomy of human behavior that has proved popular in the behavioral sciences and human factors engineering: the skill-, rule- and knowledge-based classes of performance level first articulated by Rasmussen [30], as they relate to responding to off-normal conditions. Skill-based behavior represents the behaviors that occur after an overall intention has been formed and typically take place with little conscious thought; starting a familiar item of equipment in response to an alarm is an example. Rule-based behavior comes into play when a person is aware that a problem exists and they respond using pre-formulated rules in a 'feed-forward' manner, using rules (e.g., procedures or trained strategies) as the basis for action. Knowledge-based behavior often occurs when the repertoire of rules has been exhausted, and people are forced to rely on conscious deliberative analysis, often involving trial-and-error problem solving. Slips and lapses are principally associated with failures in skill-based behaviors, and mistakes are associated with rule-based and knowledge-based behaviors.

<table>
<tr><th></th><th>Skill-based behaviors</th><th>Rule-based behaviors</th><th>Knowledge-based behaviors</th></tr>
<tr><td>Principal types of errors</td><td>Slips and lapses</td><td>Rule-based mistakes</td><td>Knowledge-based mistakes</td></tr>
<tr><td>Type of activity</td><td>Routine manual actions</td><td colspan="2">Problem-solving activities</td></tr>
<tr><td rowspan="2">Control mode</td><td colspan="2">Mainly by automated processing</td><td rowspan="2">Conscious (limited) processing</td></tr>
<tr><td>Actions</td><td>Stored rules</td></tr>
<tr><td>Predictability of errors</td><td colspan="2">Largely predictable ('strong-but wrong') errors</td><td>Variable</td></tr>
<tr><td>Ease of self-detection</td><td>Detection usually fairly rapid and effective</td><td colspan="2">Difficult and often requires external intervention</td></tr>
</table>

Table 1. Primary Characteristics and Relationships Between Different Levels of Behavior and Types of Errors (Adapted from Reason [4]).

3.2. Representation of Human Information Processing

3.2.1 Simple Model of Cognition

With the breakdown of error types and associated behavioral modes, the basis in the behavioral sciences for each type can be discussed. In order to do so, we present a simple model of human cognition (Figure 5), particularly as it relates to problem identification and solving, say, of front-line nuclear or process plant operators, airline pilots and air traffic controllers. The model (taken from NUREG-1624, Rev.1, [3]), breaks down human information processing into stages that allow analysts to address the specific types of influences that could interrupt processing during the various stages, and which correlate generally to the classes of behaviors and errors introduced above. These stages are:

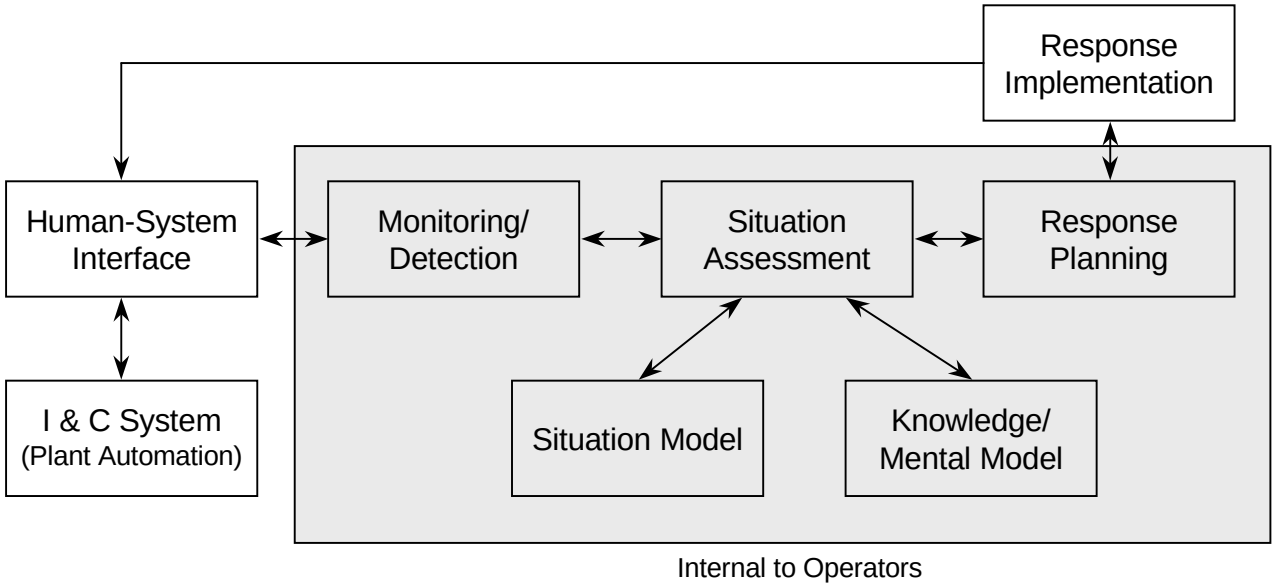


Figure 5. Major Cognitive Activities Underlying Human Performance.

- *Monitoring & detection*: This is the process by which operators become aware of the occurrence of an event by observing alarms or indications that have deviated from their expected values, and by which operators continue to monitor the behavior of the plant. Monitoring and detection actions are strongly influenced by the other information processing stages. For instance, if the operators think that a particular type of event is occurring (i.e., their situation assessment), their search for information will be very much influenced by their expectations. One particular weakness here can be the general tendency to search only for confirmatory information, not for evidence that may challenge a situation assessment.

- *Situation assessment*: This is the active process by which operators create an understanding of what is happening in the plant, in real time, based on the current inputs from the monitoring and detection activities, and based on operators knowledge and experience. Associated with situation assessment are:

    - *Situation model*: This is the operators' explanation, based on their experience and training, for what generally is happening in the plant. For example, if the event is believed to be a large loss of coolant accident (LOCA), then what *is* happening and *will* be happening in the plant, is based on the operators' knowledge and training for such events. The situation model provides a context for the operators to create the situation assessment based on current plant information, and is updated by new information from the situation assessment process.

    - *Knowledge/mental model*: The knowledge and mental models of the operators are the bases on which the operators create the situation models and awareness; they represent the basic principles and 'facts' about nuclear power plant behaviors under the ranges of conditions expected.

- *Response planning*: This stage represents the selection of appropriate actions to respond to the plant, based on the operators' situation assessment and knowledge, often in conjunction with plant procedural guidance.

- *Response implementation*: This stage represents the actual execution of the intentions formed in the response planning stage, such as the operation of equipment from the control room or the direction of the actions for operators in plant areas outside the control room.

Figure 5 provides a pictorial summary of the above stages. While it presents the processes of a single operator, it can be applied to teams where some of the functions are distributed. For example, reactor operators may accomplish the monitoring, detection and response implementation functions, and the senior reactor operator and the shift technical advisor generally fulfill (with input from the rest of the crew) the situation assessment and response planning functions.

3.2.2. Decision Making in Nuclear Power Plant Operations

In describing skill-based behavior, Rasmussen emphasized the path from the human-system interface through monitoring/detection, situation assessment, response planning and out to response implementation as virtually an automatic reaction, with little deliberative processing going on in situation assessment. Perhaps, a classical example would be the response of most experienced drivers to a red traffic signal while driving under normal conditions–there is very little assessment of the situation in terms of: "What does this indication mean? What should I do?" Rather, the errors would be more likely when red lights are located in non-normal locations that the driver has not previously experienced (as when driving in a foreign country), and, hence,

fails to see the light in time to stop, or if the location of the brake of the car is unfamiliar (relatively rare today). Other failures may be associated with interruptions in attention or distractions to the driver.

Concerning rule-based behavior, the key steps are those associated with situation assessment and response planning. Regarding situation assessment, first, several analysts in the behavioral sciences (e.g., Woods et al. [22]; Hollnagel [23]; Reason [4]; and others) have pointed out that people are most effective at identifying problems by rapid pattern matching–that is, we look at the indications of a problem and quickly select an explanation that appears to match many of the symptoms. This explanation is then used as the basis for selecting an appropriate set of responses. Once formed, this explanation can be hard to change, and hence, if wrong, gives rise to mistaken actions. With reference to the above figure, data observed by the operators is interpreted in terms of the situation model–the explanation for what is happening now. This is compared with the operator's mental model (a long-term understanding of how the plant processes work based on training and experience); in the case of rule-based behavior, this comparison is made on the basis of matching patterns of plant parameters in the actual situation versus expected patterns of expected parameter behaviors.

In rule-based behavior, the pattern matching leads the operators to select a 'standard response' (in the form of procedures or other trained actions) and to follow the actions set in the procedures. In the desire to quickly match the symptoms to a standard explanation and response, certain biases can come in to play that can lead to mistakes. Some of the most common biases that have been documented are (e.g., Reason [18]):

- recency bias–the event looks somewhat similar to a recent significant event that is in the forefront of the operators' minds, and to which they will be strongly drawn,

- frequency bias–the event looks somewhat similar to an event that occurs relatively frequently (or is used frequently in training), and is one to which operators will be drawn because of its familiarity, and

- similarity bias–the event looks like a well-known classical or standard event type that is familiar to all operators and others in the industry.

The technology used in the human-system interface can play a significant role in creating these kinds of mistakes, as discussed by Woods et al. [22], Hutchins [31], Turner & Pidgeon [32], among others. For example, the use of computer displays as the primary interface often requires accessing information serially (i.e., looking at screen after screen) so that the operators never get a complete overview. By focusing on a few parameters, the 'big picture' is lost and the biases listed above can lead the operators to a faulty (or only partially correct) assessment of the nature of the event.

In terms of response planning, in most high-hazard, low-risk industries (such as nuclear power and commercial aviation), prepared procedures are the basis for responding to off-normal

and emergency conditions. While procedures (whether written or memorized through training) provide a structured support to operators, experiments (Roth et al. [25]) have shown that they are, at best, an initial basis for action but operators must reassess the guidance in light of the actual plant conditions; even for the symptom-based procedures developed after Three Mile Island. In other words, while procedures are written using certain assumptions about the course that an off-normal condition will take, there are many opportunities for the plant to behave differently from the assumptions underlying the procedures. By simply following the letter of the procedures, the operators may inadvertently take actions that exacerbate rather than recover the conditions as a part of their response, thus creating a rule-based mistake.

Knowledge-based mistakes represent the unsafe actions that result when people have to rely on deliberative cognitive reasoning to identify and solve problems. Deliberative cognitive reasoning is not something that comes easily to people. This is because it requires adequate knowledge about the system, systematic selection and consideration of information, logical thinking, relatively high demands on memory, and can be relatively time consuming. Therefore, even in the knowledge-based behavior mode, we are limited in our processing capabilities and tend to take short cuts to identify the problem and appropriate solutions, which then underlie the potential for knowledge-based mistakes (see discussions by Woods et al. [22], Hollnagel [5, 23], and Reason [4, 18]). Examples include:

- limited short-term memory, which limits our ability to store and process more than a few items of information at any one time,
- limitations and simplifications in the mental models that are used to interpret the system's behavior, and
- limited attention resources that can lead to narrowing of the search for explanations (sometimes called 'cognitive tunneling').

Each of these effects can be exacerbated by the effects of fatigue, stress, fear, and other factors that are often the result of being challenged by a significant operational disturbance. Examples of 'real world' decision making have been studied extensively by people like Hutchins [31], Klein [33], and Klein and Salas [34]. These studies emphasize the nature of learning through experience (rather than formal education), and how the effects of ambiguity, dynamic change, and organizational pressures can degrade the effectiveness of knowledge-based performance. A recent book by Gladwell [35] presents numerous examples of both strengths and sources of failure in human performance that this kind of behavior can lead to in safety and other aspects of everyday life. The book also provides an overview of the development of our understanding of what shapes this kind of information processing in the mind.

As far as the development of several of the more recent HRA models is concerned, the focus has been on exploring issues associated with the processes shown in Figure 5, and particularly how operators can be 'set up' by plant conditions to lead to erroneous actions being taken–often referred to as errors of commission,[2] or actions that make the plant conditions worse

[2]EOC - a human failure event resulting from an overt, unsafe action that when taken, leads to a change in plant configuration with the consequence of a degraded plant state. This is in contrast with an error of omission

in the mistaken belief that they are appropriate. Using the terminology introduced earlier, these actions are mistakes that are usually the result of failures in situation assessment (though they also could result from faulty response planning, as discussed later).

Most times when operators are called on to respond to abnormal events, they are relying on rules encoded in procedures and training. These rules are largely based on expectations of plant behaviors. This is true even for the so-called symptom-based procedures that provide basic steps to be followed once certain symptoms appear, regardless of the cause of the symptoms. However, experience has shown, both in simulators and in real events, that the symptoms can mislead operators into taking the wrong actions as discussed in Roth, et al. [25]) and Kauffman [36]. During the development of the ATHEANA HRA method, several of these events were examined in detail to identify the kinds of failures that led to the wrong actions being taken (Barriere, et al. [37]). This showed that there were a set of somewhat common conditions underlying the kinds of failures seen in the events reviewed. These common conditions that can lead to unsafe actions, discussed at the beginning of this document, include:

- The plant behavior is outside its expected range
- The plant behavior is not understood
- Indications of the actual plant's state and behavior are not understood
- Prepared plans or procedures are not applicable or helpful.

When compared with the understanding of the conditions underlying mistakes, it can be seen how these match the underlying conditions described by the behavioral sciences. For instance, once parameters are outside the expected range, the process of rapid pattern matching (the normal process of situation modeling and awareness building) will not be successful, leading operators to rely on finding an alternative based on their recency and familiarity biases. If these do not lead to finding an explanation on which to act, they will typically apply knowledge-based reasoning to find an explanation, which is not always successful as discussed above. If the plant behavior or the indications themselves are not understood, the operators are led directly to knowledge-based reasoning. Additionally, if the plant procedures also are based on the expectation of the patterns of symptoms (e.g., the time sequencing of indications), this mismatch between plant behavior and plant procedures is likely to further push the operators toward using knowledge-based reasoning for their responses. While there has been considerable effort to develop procedures that do not rely on accurate interpretation of events but simply to rely on the various symptoms–the so-called symptom-based procedures– work by Roth, et al. [25], and in the development of the ATHEANA HRA method [3], shows that these procedures have many implicit assumptions concerning the time-sequencing of events and the responses required by operators. These assumed conditions and responses often represent nominal conditions. However, other time sequences can occur, suggesting that operators may face conditions where the symptom-based procedures do not match actual plant conditions, as shown in examples

---

(EOO) which is a human failure event resulting from failure to take a required action that in turn leads to a degraded plant state. Until recently, only EOOs were treated in HRA and even now, only limited evaluations of EOCs tend to be performed.

discussed in NUREG-1624, Rev. 1 [3]. As noted above, the particular processes associated with knowledge-based processing are made more difficult by such factors as stress and fatigue.

Considering the theories and understandings cited in this section, engineers 'model' human performance in a way that is directly useable in a PRA. Because PRA is foremost a failure-type model that examines undesirable events (e.g., damaging the reactor core in a nuclear power plant) involving equipment unreliability and unavailability as well as inappropriate operator actions, the discipline of human reliability analysis (HRA) has evolved in ways that attempt to utilize the above information in predicting the unreliability of operator actions associated with such events. To understand this engineering view of human performance, we now address both PRA and HRA in more detail.

4. PROBABILISTIC RISK ASSESSMENT – WHY WE WANT TO PREDICT THE LIKELIHOOD OF HUMAN ACTIONS

The driving force behind the development of HRA has been the growing use of probabilistic risk assessment (PRA) as a tool for evaluating and managing nuclear power plant safety[3]. Rather than focus on meeting a set of presumed worst credible accidents, PRA tries to look at the probability and consequences associated with all possible events (see Figure 6 for a discussion of the development of PRA). It avoids the ambiguity of defining "credible" and "incredible" events. It admits that some so-called incredible events may be more likely than chains of credible events and may have more severe consequences. It acknowledges that certain multiple failure events are more likely than some single failure events. Perhaps most importantly, it addresses the uncertainty, both aleatory (randomness) and epistemic (state of knowledge), in its data, its calculations, the success criteria for its models, and its models themselves.

Because functional failures of the nuclear power plant system depend in many ways on the performance of human operators, maintainers, and management, PRA must account for the impacts, both positive and negative, of human performance on the plant system. To support the probabilistic models and calculations of PRA, HRA must address the causes of human error and performance, the context in which unsafe acts are more likely to occur, the frequency with which such acts occur in these contextual settings, and the uncertainty in the HRA models and quantification. And this must be done in a manner consistent with the structure and sophistication of the overall PRA model.

In the following sections, we show how HRA has evolved with the growing completeness and sophistication of PRA. The evolution of methods represents expanding needs of PRA to quantitatively account for the kinds of human actions identified in examination of actual event histories and the need for PRA/HRA to be a tool for risk management as well as risk calculation.

[3]Of course, PRA and HRA have been applied to other industries and disciplines beyond safety analysis. Currently HRA methods are being expanded and specialized to support a growing number of applications in transportation (air, rail, shipping, and highway), chemical processing, defense, and homeland security.

Figure 6. The Development of Probabilistic Risk Assessment.

By the mid-1960s, the Atomic Energy Commission (AEC), whose regulatory arm later became the Nuclear Regulatory Commission (NRC), had evolved a system of safety regulation predicated on ensuring that each plant design could survive all "credible" accidents and transients, without exceeding regulatory limits for offsite exposure (DiNunno et al. [38]). The basic idea involves identifying a set of events that create the most severe, but credible, conditions for the reactor. The set includes both frequent and rare transients as well as accidents. The name of this set, as well as the philosophy used in its definition and application, changed over the years from maximum hypothetical, to maximum credible, to "design basis accidents" (DBAs).

Each design basis analysis assumed that the key event occurred followed by the single most troublesome failure of an active component. For example, a large loss of coolant accident (LOCA) was followed by the failure of one train of safety injection (the water supply designed to maintain coolant inventory in case of such an accident). Rather sophisticated criteria for selecting the most limiting conditions (time in life, temperature, pressure, etc.) and for evaluating success were published in the regulations (for example, see any final safety analysis report [FSAR] from a nuclear power plant).

Nevertheless, a number of concerns led the AEC and others to wonder if there were gaps or unnecessary burdens in our regulations; for example:

- the DBA and single failure criterion were almost surely overly protective in some areas
- on the other hand, some scenarios with multiple failures might be more likely than the single failure case of the DBA
- could some "incredible" events outside the safety analysis be more likely and more severe than some included events; for example, were there conditions in which failure of the reactor vessel would be more likely than the double-ended break of a large pipe
- what would happen if the unlikely occurred and the plant reached a beyond-design-basis condition
- with growing numbers of reactors, even low probability events could accumulate to significant public risk

As a rough cut consideration of the possibility that beyond-design-basis events constituted a significant risk, a report analyzed the potential effects of a set of mutually impossible "worst case" conditions [e.g., 100% of all fission products within the core distributed throughout the containment (direct gamma shine at the site boundary), 100% of volatile fission products released from the containment (direct shine to the public and washed out for the contamination dose)] (WASH-740 [39]). A caveat in the report stated that 'the significance of damages consequent to accidents cannot be appraised independently of the probability of the accident.' They believed the probability of a hazardous accident to be exceedingly small, but did not see how to estimate it. They did put some perspective on the possible consequences of such events."

By the late 1960s, a combination of concerns about the existing approach to regulation and improved capabilities in reliability analysis developed in the aerospace and chemical industries combined to spur the AEC to commission the first large-scale use of PRA. The *Reactor Safety Study* (Rasmussen et al. [40]), commonly known as the Rasmussen Report and WASH-1400 [40], was the result. It extended existing reliability methods and developed a very successful structure, the event tree on critical safety functions to organize the model. This structure transformed an originally intractable large fault tree into a set of initiating events and subsequent safety system response fault trees that allowed review and checking against previous analyses, as well as facilitated a very complex calculation. That structure continues to serve the needs of nuclear plant systems analysis very well. Alternative structures have proved valuable in other applications.

The basic approach of the *Reactor Safety Study* has proved durable and effective and the study set standards in many areas of safety analysis. However, little was available to support modeling of human actions and human errors at the time of the study. The authors argued that on the whole they believed that the positive effects of human operators probably out-weighed the negative aspects of human error (Congressional Testimony [41]). Some simple models and quantification were included. Later reviews criticized the lack of thorough modeling of human error (Lewis et al. [42]) and made it clear that work was required to develop an HRA capability consistent with the state-of-the-art in modeling systems performance. Of course human error was not the only area requiring more sophistication.

4.1. The Role of HRA in PRA

HRA is a critical component of PRA. PRA models systems' performance and their ability to provide safety related critical functions. In spite of the fact that in many systems, such as nuclear power plants and airplane cockpits, safety related functions are sometimes automatically initiated, there are still many situations where operator control is necessary and situations where operators decide to take manual control. Thus, an important aspect of a PRA is to appropriately model human actions that are needed to ensure critical functions or that could cause the loss of a critical function (including maintenance and testing related human actions that could render a system unavailable when needed). In other words, the overall objective of HRA in a PRA is to include the impacts of personnel actions in an assessment of risk.

Generally, there are three broad classes of human actions relevant to a PRA: routine actions (including unscheduled maintenance), actions that lead to the initiation of an accident scenario, and actions that occur during the evolution of the accident sequence. In nuclear power plant PRA, these are historically referred to as pre-initiator, initiator, and post-initiator human actions, respectively.

Routine and unscheduled maintenance actions that are modeled include such latent errors as miscalibrations of instruments and failures to restore equipment after test or maintenance. These latent errors are not usually important contributors to the loss of equipment, because many of these failures are easily recovered and modern post-maintenance test requirements make it unlikely that maintenance errors survive into the operating mode. However, as new methods dig deeper into the causes of unsafe acts during the accident sequence, it is expected that the cognitive difficulties introduced by unexpected conditions caused by latent errors may be found to be important to risk. As discussed earlier, given the important role of latent errors in many serious accidents, it appears that their impact on crew response in accident scenarios should be considered in the PRA if a realistic assessment of risk is required.

In addition, although human actions that initiate an accident scenario have not traditionally been modeled in PRA (the experience-based initiating event frequencies usually include their contribution), such scenarios at least have the potential to create problems for crew response. For example, the source of the problem might be unexpected, and therefore potentially confusing. There are special cases and certain technologies for which explicit HRA treatment of human-induced initiators is necessary.

The main focus of most PRAs, however, usually is human actions that occur during the accident sequence. To include such human actions realistically in the PRA, the modeling of human interactions considers each action evaluated in the context of a complete accident scenario. In the early days of PRA, accident sequence analysts simply provided the human events of interest to a HRA specialist who then assigned human error probabilities (HEPs) to the human events, often in isolation from the rest of the PRA team. Such a process is no longer considered good practice. Current good practice in HRA requires inputs from a team of personnel, representing multiple disciplines, in order to perform the three major aspects of HRA:

1) identify accident scenario contexts and associated human actions, 2) quantify the probabilities of failure of each relevant human action (while considering the context, including plant conditions and other important factors that can influence performance), and 3) when necessary, identify ways to improve human performance and avoid important unsafe actions. It should be noted that standards for accomplishing the major aspects of HRA have been developed in recent years (ASME [43]; IEEE [44]) and the U.S. Nuclear Regulatory Commission (USNRC) has developed guidance (HRA good practices) for how to meet such standards (NUREG-1792 [45]).

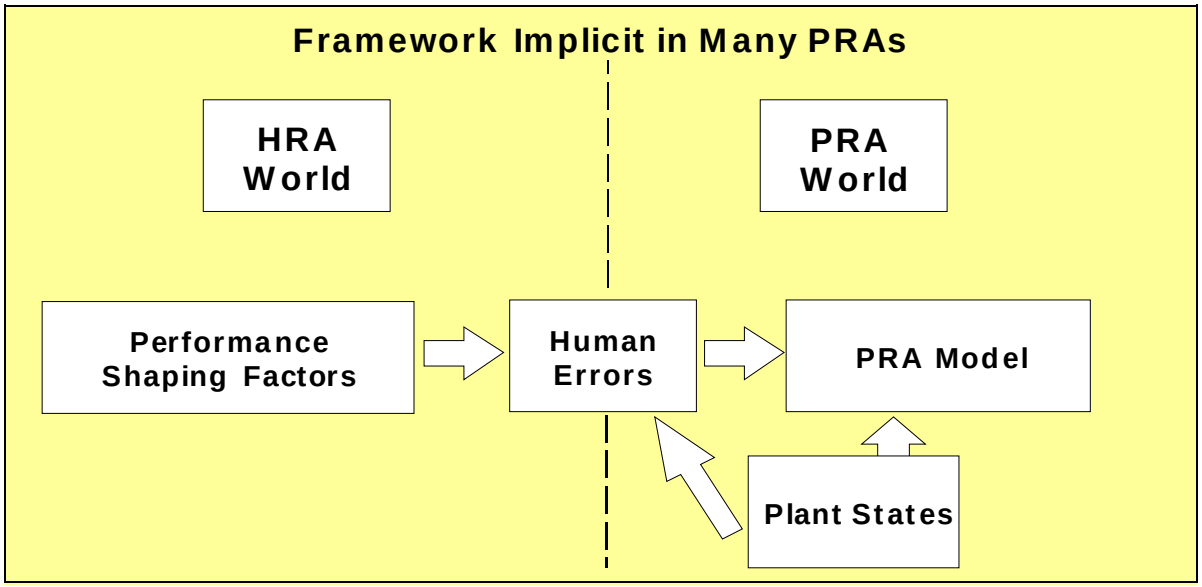


Figure 7. Framework Implicit in Many Earlier HRAs.

The two framework charts (Figures 7 and 8) illustrate representations of the earlier and the more current frameworks, respectively, for the relationship between PRA and HRA. The multi-disciplinary, integrated approach, with expertise in facility operations and training, facility engineering, PRA and behavioral science, is needed because understanding an accident scenario context is a complex, multi-faceted process (from the ATHEANA HRA method [3]). The interaction of facility (for example, airplane) hardware response and the response of operators (e.g., pilots) must be investigated and modeled accordingly. The following are examples of characteristics (among many other characteristics), that must be understood and reflected, as necessary, in a model of a specific human action or group of human actions:

Multidisciplinary HRA Framework

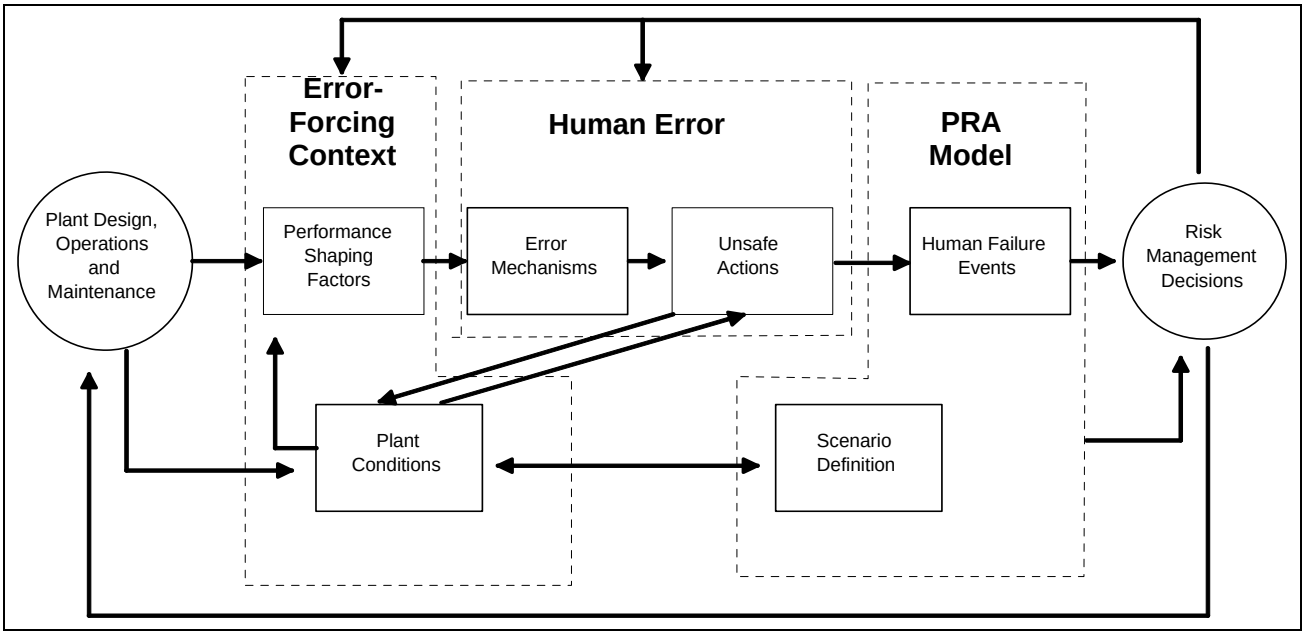


Figure 8. Multidisciplinary HRA Framework from ATHEANA (NUREG-1624, Rev. 1[3]).

- the timing of events and the occurrence of human action cues,
- the parameter indications used by the operators and changes in those parameters as the scenario proceeds,
- the time available and locations necessary to take the human actions,
- the equipment available for use by the operators based on the scenario,
- the environmental conditions under which the decision to act must be made and the actual response must be performed,
- the degree of training guidance and procedure applicability, and
- the way the crews interact with one another and implement the procedures.

Hence, to model human actions in the PRA (e.g., in a nuclear power plant PRA), PRA and HRA practitioners, thermal-hydraulic analysts, operations, training, and maintenance personnel, and sometimes other disciplines depending on the accident scenario (e.g., structural engineers might be needed if the timing of an action is dependent on when and how the containment might fail) all can have input into defining as well as quantifying the probabilities of human actions to be included in the PRA. Each discipline provides a portion of the context knowledge. Only when the context is sufficiently understood can the human action event be realistically modeled and quantified. In addition, good practice in HRA (see NUREG-1792 [45]) includes the use of tools or information sources such as task analysis, simulator exercises, field observations, walk downs of areas where the action needs to take place, and talk-throughs of the scenario and actions of interest with plant operators or maintenance personnel. For a thorough

PRA, it is not good practice to perform a human reliability assessment “sitting in an office” with little or no interaction with those who can provide an understanding of the scenario context.

It should be noted that even when all of the information described above has been collected in performing the HRA and the scenario context has been thoroughly documented, analysts must then determine how to combine all of the information in order to obtain estimates of the probabilities of the unsafe actions. Moreover, as the discussions in the sections above on the perspectives from the behavioral sciences and from the examination of operational events illustrate, there are numerous ways in which the context can occur and evolve, and then interact with the characteristics of human information processing to create opportunities for unsafe acts to occur. An important aspect of the evolution of HRA technology has been the need to better account for the wide range of factors and conditions that have been identified over the years as having strong influences on human behavior.

4.2. Evolution of HRA Technology

Human reliability analysis (HRA) methods have evolved along with the practice of HRA as is discussed in the previous section. Figure 9 provides an overview of the evolution of HRA methods (see Table 2 below for the citations for the various methods) and some of the more influencing events that have stimulated this evolutionary process. Besides the timing of each method, Table 2 (discussed in more detail later) provides a cataloging of HRA methods from two viewpoints; the general focus of each method and the quantification process employed to estimate human error probabilities (HEPs). Collectively, these views of the evolution of HRA technology and methods help us to understand the current status of HRA. Additional overviews of many of the methods are provided by Swain [46], Gertman and Blackman [8], and Hollnagel [5] for the methods commonly in use at the time. The most recent review of available methods (covering ten methods used in the U.S.), including discussions of their strengths, weaknesses, and applicability can be found in NUREG - 1842 [47].

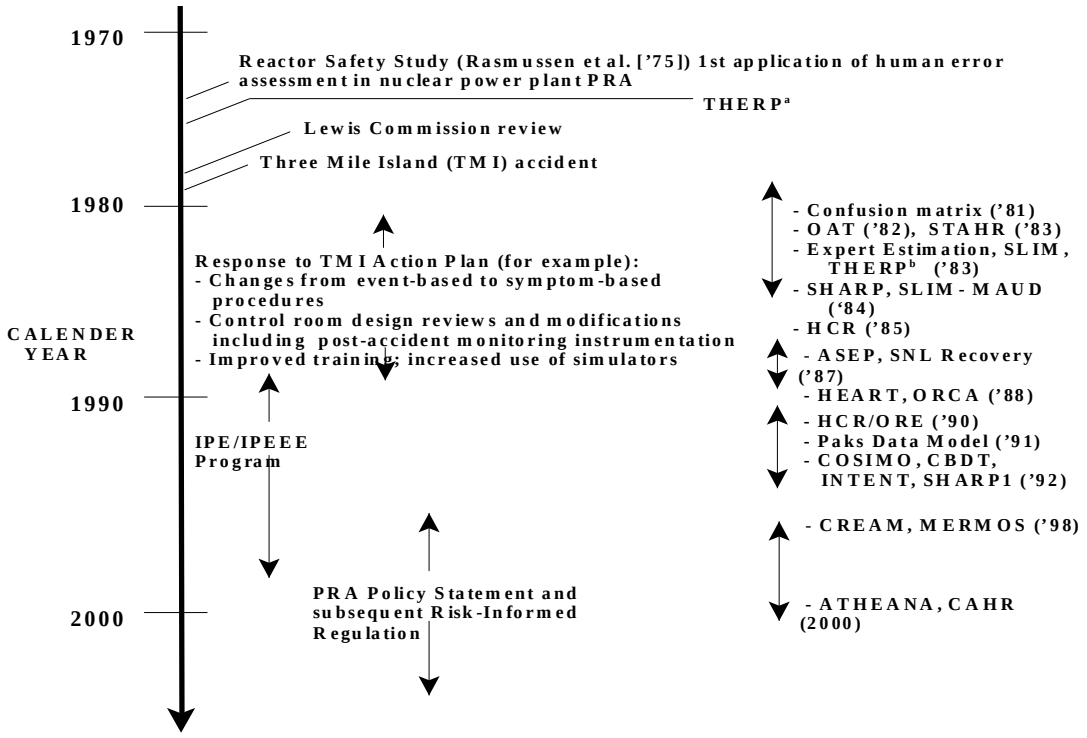


Figure 9. Time History of HRA Methods[c] Development.

[a] THERP[a] refers to the version of THERP (Swain and Guttmann [13]) used in the Reactor Safety Study (Rasmussen et al. [40]) and which was documented in that study's final report. THERP[1] involved simple modeling of what we today call slips and lapses, such as missing a step in a procedure.
[b] THERP[b] (Swain and Guttmann [13]) refers to the detailed HRA method documented in NUREG/CR-1278.
[c] See Table 2 for citations for the various methods.

4.2.1. Time Evolution of HRA Methods

Figure 9 provides a time history of HRA methods development. There have been a number of events that have affected the evolution of HRA methods. Some of this evolution has been in response to the demands of and the parallel maturing of PRA; other HRA method evolution influences have been actual events and subsequent activities in response to those events. The figure shows some of the more prominent influences on HRA over the past thirty years.

Table 2. Summary of the General Focus of Each HRA Method and its Approach for Quantification.

Focus of HRA Method	Approach for Quantification
THERP[1] (as documented in Rasmussen, 1975 [40]) -original form of THERP (Swain and Guttmann, 1983 [13]); primarily modeled aspects such as missing a step in procedure, reading a wrong indication, selecting a wrong switch, etc.	Provides tabulated failure estimates
Confusion Matrix (Potash et al.,1981 [51]) - models mis-diagnosis; e.g., confusing event 'A' as event 'B' because of similarities	Expert judgment
OAT (Hall et al.,1982 [15]) - considers that with greater time for diagnosis, there is an increased likelihood of detecting and correcting mistakes	Provides tabulated, time-reliability based failure estimates
THERP[2] (Swain and Guttmann,1983 [13]) - adds to the original version of THERP, the ability to estimate diagnostic errors within periods of time	Provides tabulated or time-reliability based failure estimates
STAHR (Phillips et al., 1983 [52]) - estimates the effects of different (user-identified) factors on the overall likelihood of human error	Expert judgment
Expert Estimation (Swain and Guttmann, 1983 [13]) - uses a set of techniques to elicit expert judgments, mainly for diagnostic errors	Expert judgment
SLIM (Embrey, 1983 [53]) - provides a calculation process to estimate the overall likelihood of an error based on a range of user-identified performance shaping factors. In principle can be applied to any type of error	Expert judgment along with a mathematical formula for combining judgments
HCR (Hannaman et al.,1985 [54]) - estimates the likelihood of failure based on data gathered for response times for similar actions in simulators. Focus is on non-response probability	Ideally derives time-reliability based estimates from plant specific simulator exercises, but may use expert judgment to obtain time-reliability parameters. Some tabulated model parameters provided to reflect effects of a few PSFs.

SLIM-MAUD (Embrey et al., 1984 [55]) - a variant of SLIM and provides additional tools for comparing the effects of different performance shaping factors	Expert judgment along with a mathematical formula for combining judgments
SHARP (Hannaman and Spurgin, 1984 [56]) and SHARP1 (Wakefield et al., 1992 [57]) - Frameworks for performing HRA, but not quantification tools	No explicit quantification process, but methods available at the time were discussed
ASEP (Swain, 1987 [58]) - a variant of THERP[1 & 2] (Swain and Guttmann, 1983 [13]) using a more explicit process suitable for non-HRA experts and reduces the number of factors to be considered	Provides tabulated or time-reliability based failure estimates
SNL Recovery Model (Whitehead, 1987 [59]) - provides sets of time-reliability models to estimate error probabilities resulting from mistakes and failure to respond correctly	Time-reliability based failure estimates to be extrapolated from the model data to the specific application
HEART (Williams, 1988 [60]) - provides a generic set of descriptions of types of tasks and factors that influence the overall probability of failure	Tabulated data mathematically combined to reflect the type of task and PSFs
ORCA (Dougherty and Fragola, 1988 [17]) - provides tools for estimating errors including a THERP-like approach for slips/lapses and time-reliability relationships with a small number of factors considered in estimating HEPs for mistakes	Provides tabulated or time-reliability based failure estimates
HCR/ORE (Spurgin, et al., 1990 [61]) - revision of HCR that provides estimates of failure(non-response probability) based on simulator data or expert judgment and assumptions regarding applicability of normal distribution	Ideally derives time-reliability based estimates from plant specific simulator exercises, but may use expert judgment to obtain time-reliability parameters
INTENT (Gertman et al., 1992 [62]) - estimates mistakes based on historical experience of power plants as reported to NRC and other HRA/PRA estimates	Some empirical data along with expert judgment
CBDT (Parry et al.1992 [63]) - a follow-on to HCR and HCR/ORE, allows the estimate of error probabilities for conditions involving longer time scales and considers causes of errors as opposed to time-reliability relationships	"Tabulated" failure estimates through application of decision trees

COSIMO (Cacciabue et al.,1992 [64]) - uses computer simulation of the human diagnosis and decision making processes in combination with a model of plant processes	Expert judgment
Paks Data Model (Bareith et al., 1996 [65]) - uses data based on extensive analysis of one plant's simulator data	Plant simulator data
CREAM (Hollnagel,1998 [5]) - estimates relative likelihoods of failure based on overall representations of contexts including consideration of workplace, task, and organizational factors	Provides tabulated failure estimates
MERMOS (Bieder et al.,1998 [50]) - provides a way of modeling errors in the integrated human team-computer environments in advanced control rooms using observations of errors in simulator exercises	Expert judgment primarily, but may use some plant data (simulator or operational) as one basis for the estimation process
ATHEANA (NUREG-1624, Rev. 1, 2000 [3]) - searches for conditions (contexts) in which mistakes are likely and then considers the likelihood of those contexts. Later development of the use of expert opinion to determine the likelihood of making the mistake	Expert judgment
CAHR (Strater, 2000 [25]) - estimates the likelihood of different types of errors based on the analysis of actual events and the contexts in which they occurred including the frequencies of error contributing factors	Use some plant data (simulator or operational) as one basis for the estimation process–however, the final quantification uses judgment for the specific error probabilities.
SPAR-H (Gertman et al., 2005 [66])-similar to THERP, includes slips, lapses, and mistakes and addresses diagnosis and response execution through use of several PSFs as multipliers. Not intended for detailed analysis of decision-making	Provides tabulated failure estimates

As the first comprehensive nuclear power plant PRA, the Reactor Safety Study (Rasmussen et al. [40] was focused on plant hardware but recognized that some potential accidents could be significantly affected by whether the operators failed to perform certain actions. In attempting to include the effects of these actions in the PRA, the analysts did not find either available methods or experts willing to address questions that needed to be answered, such as whether the operators would fail to initiate the recirculation cooling mode of emergency core cooling following a

LOCA. Nevertheless, probabilities were supplied for a few cases all using the form “What is the probability that the operators fail to____?”

A subsequent review of that first PRA by the Lewis Commission [42] identified four fundamental limitations in the method used, including:

- insufficient data,
- methodological issues associated with time-scale limitations,
- omission of the possibility that operators may perform recovery actions, and
- uncertainty regarding the actual behavior of people during accident conditions.

Just six months following the Lewis Commission report and before there could be much reaction to its findings, the Three Mile Island (TMI) accident occurred in March 1979. Unsafe human action was a critical element of what went wrong at TMI, and involved a misunderstanding of actual plant conditions and the subsequent inappropriate shutdown of all injection into the reactor coolant system by the operating crew. Following that event, during much of the next decade and, especially during the five years immediately following the accident, both the NRC and the industry made numerous changes as part of the many lessons learned from the accident. Most notably related to the field of HRA, the industry changed from using event-based emergency operating procedures (EOPs) to symptom-based EOPs to avoid operators from having to diagnose what the event was at the start of an event. Instead, operators could simply respond to indications of key parameters (levels, pressures, temperatures, etc.) so that safety was ultimately achieved by ensuring these parameters stayed in or were brought back within acceptable ranges by performing various actions with available equipment. Further, control room design reviews were held and improvements were made in the indications and their layout in the control rooms so as to lessen the chance of confusion as to the status of plant conditions during any abnormal situation. In step with both these changes, more training of operators was enacted to better inform them of conditions that could lead to a severe accident. Also, upgrading and more wide-spread use of plant simulators to instruct operators about challenging events was begun.

Paralleling these activities in response to TMI, along with considerable study of the potential for severe accidents in nuclear power plants, the field of HRA saw a series of HRA methods developed that were much more focused on analyzing the likelihood of operators making mistakes (i.e., addressing the TMI experience) and related diagnosis errors, rather than the simpler slips and lapses. Much of this methods development took advantage of the types of advances made in the behavioral sciences summarized earlier. More on the main characteristics of these HRA methods is provided later. Nevertheless, it became increasingly critical to understand and model operator mistakes and related unsafe actions since, as part of the TMI aftermath, plants were making hardware changes that made the plants more robust. Hence, human unsafe acts became more significant to risk since operators could still defeat the increased diversity and redundancy. This became evident as the Individual Plant Examination and to some extent the Individual Plant Examination for External Events (IPE/IPEEE) programs were implemented, whereby all plants performed detailed PRAs of their plants to understand the

potential vulnerabilities to severe accidents on a plant-specific basis. With the increasing detailed demands of these PRAs, more sophistication was required in the HRA methods and tools to assess the potential risks associated with operator unsafe acts during abnormal and accident situations. The change to a more risk-informed regulatory process has further increased the demands of modeling human performance as realistically as necessary to be able to address specific questions regarding the risk impact of plant changes including changes in operational practices. HRA methods development has continued to respond to these increasing demands.

4.2.2. General Focus of HRA Methods and Approach for Quantification Process

The HRA methods noted in Figure 9 vary in terms of their general focus (e.g., the type of errors addressed, consideration of decision-making) and in terms of the general approach they use for quantifying human failure events (HFEs) for a PRA, among other aspects. The general focus of the methods reflect, at least to some extent, the evolving knowledge-base of HRA (e.g., the need to better address the decision-making process), while the different approaches to quantification reflect more pragmatic concerns (e.g., ease of use), and tend to be represented all along the temporal continuum. Table 2 provides a list of the different methods that have been developed over the years (may not be a complete list) and discusses their general focus and their general approach to quantification. More detailed discussions of ten of these methods that have frequently been used in the U.S. can be found in NUREG-1842 [47].

As mentioned above and noted in Table 2, following the earliest work on the simplest of errors (i.e., slips and lapses), considerable expansion occurred to create methods that would address either mistakes like those performed at TMI, or generally all types of errors, within the method framework. Another issue was the extent to which earlier methods tended to consider a safety related human action to be similar to an item of equipment that either succeeds or fails in its intended function. That is, while a few factors may be taken into account by the methods in estimating the likelihood of failure to take the action, the analysis focuses on just the success or failure of actions typically defined by systems analysts as important to safety.

Many analysts, particularly those trained in the behavioral sciences have criticized this approach as gravely over-simplistic (e.g., Woods et al. [16]; Dougherty [48]; Hollnagel [5]). Even NRC's review of HRA in NUREG-1050 [49] identified the limitations in the earlier methods as an important weakness in PRA. Many of the more recent HRA models recognize that people behave in very complex ways and are capable of creating new conditions (not simply failing to accomplish system-demanded tasks) or are subject to influences in more complex ways than those implied by a few simple performance shaping factors. The development of some of the most recent methods incorporates explicitly some kind of a model of human cognitive behavior that takes account of the knowledge of the behavioral sciences, to provide a much richer description of the human-system interactions. By taking account more realistically of the cognitive processes of the operators, it is possible to be much more explicit about the kinds of conditions, or *contexts*, that are necessary to lead to high likelihood of failure, or may induce unsafe actions by operators. This came about because when analysts more closely examined real-

world event data especially in light of the advances in behavioral science and theories about how humans function, it was found that the more serious accidents involved:

- the plant operating outside normal or expected conditions,
- the resulting physical regime not being well understood by the operators,
- operators refusing to believe or otherwise recognize evidence contrary to their belief as to what was happening in the plant, and
- prepared plans were not always helpful or even applicable.

Hence, it was recognized that HRA methods needed to holistically account for both plant conditions and a widening range of operator influences (i.e., performance shaping factors) in order to be able to address the characteristics of the more serious accidents. While not perfect, some of the more recent methods provide considerable guidance on understanding, as much as possible, about the *whole context* of a situation faced by the operators in order to estimate the likelihood of operator unsafe acts. In some cases, this expanded understanding also includes more explicit treatment of errors of commission (EOCs). Even so, advancements are still needed to be able to address the potential impact of management and organizational influences, and the role of crew characteristics and team dynamics on crew performance. Additionally, more analysis of operational and simulator experience is needed in order to add credibility to the methods and particularly the likelihoods of operator errors as estimated using these methods.

With respect to the basis for quantification, there are generally three different bases (see Table 2 for examples of each):

- the method provides a numerical basis, such as HEP values that are tabulated or expressed in a time/reliability relationship (this may, in turn, be based on actual experience, simulator observations, judgment, etc.)

- the method provides ways to elicit or manipulate expert judgment

- the method provides ways to obtain data from plant-specific data sources (such as simulators).

While in some cases, the method may use somewhat of a mixture of the bases shown, the predominant mechanism by which human error probabilities are quantified is shown in Table 2.

It is noticeable that most of the more recent HRA methods rely on some form of expert judgment, whereas the majority of the earlier methods rely on tabulated or time reliability based failure estimates. One reason for this difference is that the effects of contexts considered in more recent methods like CREAM [5], ATHEANA[3] and MERMOS[50] is much more complex and not readily reducible to simple tables or correlations using a few performance shaping factors. Hence, while the use of simple tables, correlations, and related multiplicative factors make the earlier methods somewhat easier to use, the simplicity of the methods that allowed the use of such approaches was in fact one of the primary criticisms of them that led to evolution of HRA models.

4.2.3 Summary of Evolution of HRA

The evolution of HRA technology and the methods for evaluating human performance and estimating human error probabilities associated with nuclear power plant applications has occurred consistently over the past thirty years. In large part, this evolution has been in response to our needs to understand the drivers of human performance in increasing detail, as well as in response to changes in the industry and due to the ability to incorporate our knowledge from the behavioral sciences. Simple modeling and quantitative techniques were and continue to be useful for simpler types of human errors (and, hence, are still used today). However, as we improve the man-machine interfaces in our nuclear plants, it has become increasingly important to understand and model the more cognitive aspects of human performance within the context of situations that operators may experience during abnormal events and in accidents. This has required more complex and sophisticated modeling as well as more reliance on expert elicitation quantitative techniques. These advances reflect our improving ability to understand and predict human behavior in challenging situations. Nevertheless, not all known factors are yet routinely and completely addressed in the current HRA methods (e.g., organizational influences). Also, while analysts generally believe the quantitative estimates are reasonable, HRA is still struggling to obtain and use sufficient real world experience to "gauge" the accuracy of our HEPs. Since serious challenges to operator performance tend to be rare (which is fortunate), such data is slow in coming and it will take time to be able to validate our quantitative estimation techniques.

5. CAN WE PREDICT UNSAFE HUMAN ACTIONS AND THEIR LIKELIHOODS?

The short answer is yes, we can, but some discussion is needed. Our current human reliability modeling techniques have become far more sophisticated and, generally, can account for many more influences on human performance than was available with the earliest methods. Taking into account the advances in the behavioral sciences in our current models, we believe it is possible to identify those situations that tend to make human error more likely. This allows us to define potential vulnerabilities and make improvements in plant design and operational practices, as well as in procedures and operator training that collectively, can lessen the chances of unsafe human actions.

There are many HRA methods giving human reliability analysts an arsenal of tools for identifying conditions prone to operators making unsafe acts. Some methods and their tools treat human performance relatively simply and account for only a few influencing factors. Such treatment may be adequate for situations that are not complex and when the most likely influencing factors are within the capabilities of the method. Other methods involve more complex modeling of human performance, and are most useful and probably necessary for conditions requiring consideration of many influencing factors. Although the USNRC has recently provided some guidance on the appropriate use of various types of HRA methods [47],

knowing when to use as well as how to use a method is part of the "art" of HRA and requires a sufficiently trained analyst to make the appropriate judgments required by any of the methods.

The methods also have their associated means for quantifying the likelihood of operators performing unsafe actions. These range from the simple use of data tables (that are based on experience and judgment) to more complex expert elicitation processes (that, preferably, use personnel knowledgeable in the tasks being examined). While there is the belief that these quantification techniques generally provide reasonable probabilities if applied correctly and to the right situations, all of HRA still suffers from having too little relevant experience to "calibrate" or otherwise validate these quantification techniques. Efforts continue to make such data (and analysis of the data) available along with the need to improve our modeling of human performance so as to handle yet additional performance shaping factors such as organizational influences.

Thus, the state-of-the-art in HRA is such that we believe we can identify conditions that tend to make errors more likely and estimate "reasonable" probabilities for the errors. This should not be confused, however, with being able to predict the next critical human error. Just as we know that the probability of getting a "head" when flipping a coin is 0.5, that does not mean we can predict whether or not the next flip of a coin will produce a "head", or even the flip after that or after that. We can say that given a sufficient number of flips, you will see a "head" 50% of the time. In a more complex example, we cannot predict the specific paths of neutrons during nuclear fission and whether specific neutrons will cause other fissions of uranium nuclei. But, we know "on average" what will happen and this is sufficient for us to be able to design and build operating reactors.

It is the same with our human reliability predictions. For a case where we estimate a high probability of failure by the operators, that probability is a reflection of various influencing factors that given the situation, we believe tend to make human error likely. In such cases, the most negative influences can be defined and improvements made to lessen the chance of an unsafe action. Conversely, a low probability is a reflection of all the positive influences that exist for the situation that should make a human error unlikely. Such results are useful, even if we cannot predict that given a particular circumstance and the related influences, that an error will or will not occur.

Clearly, further advances in the field of HRA are needed. It is not clear that the behavioral sciences will be able to produce an adequate integrated model of human performance to support direct quantification of HFEs. Therefore, the systematic collection of a "database" (or information source) of operational events and simulator experience to support HRA quantification would seem to be a very high priority. Such a database should be made up of national and international data, collected on actual events across the different industries, and from investigations using simulators. Such data will continue to strengthen our ability to understand the characteristics of situations that can lead to unsafe human actions and provide an additional basis for estimating the likelihood of those unsafe actions. The USNRC is currently supporting several national and

international efforts along these lines, including work at the Halden Research Project in Norway using state-of-the-art nuclear power plant simulators, the international Organization for Economic Cooperation and Development Nuclear Energy Agency (OECD/NEA) efforts to develop an international database of nuclear power plants events, and work by Idaho National Laboratory to build a structured database for collecting information associated with unsafe human actions that could be used to support quantification (e, g., Hallbert et al. [67]).

In the meantime, HRA provides us with useful insights and allows us to make meaningful improvements to lessen the likelihood that unsafe actions will occur.

6. REFERENCES

[1] Gitus, J. H. *The Chernobyl accident and its consequences.* London, United KingdomAtomic Energy Authority, 1988.

[2] *Air Florida, Inc., Boeing 737-222, N62AF, Collision with 14th Street Bridge, near Washington Nat'l Airport, Washington, DC, January 13, 1982.* National Transportation Safety Board Report Number: AAR-82-08, Washington DC, USA, 1982.

[3] *Technical basis and implementation guidelines for A Technique for Human Event Analysis (ATHEANA),* NUREG-1624, Rev. 1, US Nuclear Regulatory Commission, Washington, D.C., May 2000.

[4] Reason, J. *Human error*. Cambridge, Cambridge University Press, 1990.

[5] Hollnagel, E. *Cognitive reliability and error analysis method (CREAM)*. York: Elsevier Science, New York, 1998.

[6] *An analysis of root cause failures in 1983 significant event reports.* INPO 84-027, Atlanta, GA: Institute of Nuclear Power Operations, 1984.

[7] *A maintenance analysis of 1983 significant events.* Atlanta, GA: Institute of Nuclear Power Operations, 1985.

[8] Gertman, D.I. and Blackman, H.S., *Human reliability and safety analysis data handbook,* John Wiley & Sons, 1994.

[9] Reason, J. *Managing the risks of organizational accidents*. Ashgate Publishing Company, Brookfield, Vermont, 1997.

[10] Kletz, T.A. *What went wrong? Case histories of process plant disasters*, Gulf Publishing Co., London,1985.

[11] Dekker, S. *The field guide to human error investigations,* 2002 Ashgate Publishing Co., 2002.

[12] Harré, R., and Lamb, R. (Eds.). *The Encyclopedic Dictionary of Psychology*. Cambridge, MA: MIT Press; 1983.

[13] Swain, A.D., and Guttmann, H.E. *Handbook of human reliability analysis with emphasis on nuclear power plant applications - final report,* NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, August 1983.

[14] Rasmussen, J., and Rouse, W.B. *Human Detection and Diagnosis of System Failures*, New York: Plenum Press, 1981.

[15] Hall, R.E., Fragola, J. and Wreathall, J. *Post event human decision errors: Operator action tree/time reliability correlation*, NUREG/CR-3010, U.S. Nuclear Regulatory Commission, Washington, 1982.

[16] Woods, D.D., Roth, E.M., and Hanes, L.F. *Models of Cognitive Behavior in Nuclear Power Plant Personnel*, Westinghouse Science & Technology Center, Pittsburgh, PA NUREG/CR-4532, July 1986.

[17] Dougherty, E.M., and Fragola, J.R. *Human reliability analysis. A systems engineering approach with nuclear power plant applications*, New York, John Wiley and Sons, 1988.

[18] Reason, J. The Review of Mistakes: A Brief View of Planning Failures. In: Rasmussen J, Duncan K, Leplat J, eds. *New Technology and Human Error*. New York: John Wiley & Sons; 1987.

[19] Minsky, M. A framework for representing knowledge, In P. Winston (Ed.), *The Psychology of Computer Vision.* New York:McGraw-Hill, 1975.

[20] Rumelhart, D.E. Notes on a schema for stories. In D. Bobrow and A. Collins (Eds.) *Representation and Understanding: Studies in Cognitive Science.* New York: Academic Press, 1975.

[21] Tversky, A., and Kahneman, D. Judgment under uncertainty: Heuristics and biases. *Science, Vol. 185*, pp 1124-1131, 1974.

[21] Woods, D.D., Johannesen, L.J, Cook, R.I., and Sarter, N.B. *Behind Human Error: Cognitive Systems, Computers, and Hindsight*. Wright-Patterson Air Force Base, OH: Crew System Ergonomics Information Analysis Center; 1994.

[23] Hollnagel, E. *Human Reliability Analysis: Context and Control.* San Diego, CA: Academic Press, Inc., 1993.

[24] Hollnagel, E. *Reliability of Cognition: Foundations of Human Reliability Analysis.* New York: Basic Books, 1994.

[25] Roth, E.M., Mumaw, R.J., and Lewis, P.M. *An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies*. Report No. NUREG/CR-6208. Pittsburgh, PA: Westinghouse Science & Technology Center; July 1994.

[26] Sträter, O. *Evaluation of human reliability on the basis of operational experience*. GRS-170, Koln Germany: 2000.

[27] Sträter, O, and Bubb, H. “Design of Systems in Settings with Remote Access to Cognitive Performance,” In Hollnagel, E. and Suparamaniam, N. (Eds.) *Handbook of Cognitive Task Design*, Lawrence Erlbaum, Hillsdale, 2003.

[28] Norman, D.A. *Categorization of action slips*. Psychological Review 1981; 88:1-15.

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

[30] Rasmussen, J. “Skills, rules, knowledge: signals, signs and symbols and other distinctions in human performance models,” *IEEE Transactions: Systems, Man, and Cybernetics*, 1983, SMC-13,257 -267.

[31] Hutchins, E. *Cognition in the Wild*. Cambridge: MIT Press; 1995.

[32] Turner, B.A, and Pidgeon, N.F. *Man-made Disasters*. Second ed. Boston: Butterworth-Heinemann; 1997.

[33] Klein, G.A., *Sources of Power: How People Make Decisions*, Cambridge, MA: MIT Press; 1999.

[34] Klein, G.A., and Salas, E. *Linking Expertise and Natural Decision Making*. Mahwah, NJ: Lawrence Erlbaum Associates; 2001.

[35] Gladwell, M., *Blink: The Power of Thinking Without Thinking*. New York: Little, Brown & Co., 2005.

[36] Kauffman, J.V. *Engineering Evaluation: Operating Events with Inappropriate Bypass or Defeat of Engineered Safety Features.* Washington, DC: Office for Analysis and Evaluation of Operational Data, U.S. Nuclear Regulatory Commission, 1995.

[37] Barriere, M.T., Wreathall, J., Cooper, S.E., Bley, D.C., Luckas, W.J., Ramey-Smith, A. *Multidisciplinary Framework for Human Reliability Analysis with an Application to Errors of Commission and Dependencies*. NUREG/CR-6265, BNL-NUREG-52431. Upton, NY: Brookhaven National Laboratory, 1995.

[38] DiNunno**,** J.J., Anderson, F., Baker, R., and Waterfield, R. *Calculation of distance factors for power and test reactor sites,* U.S. Atomic Energy Commission report TID-14844, March 1962.

[39] *Theoretical possibilities and consequences of major accidents in large nuclear power plants,* WASH-740, U.S. Atomic Energy Commission, 1957.

[40] Rasmussen, N.C., et al., *The reactor safety study,* WASH-1400 (NUREG-75-014), U.S. Nuclear Regulatory Commission, Washington, D.C., 1975.

[41] Congressional Testimony. *Reactor safety study (Rasmussen report), oversight hearings before the subcommittee on energy and the environment of the committee on interior and insular affairs,* House of Representatives, Ninety Fourth Congress, Second Session, Serial No. 94-61, Washington D.C., June 11, 1976.

[42] Lewis, H.W., et al. *Risk assessment review group report to the U.S. Nuclear Regulatory Commission,* NUREG/CR-0400, U.S. Nuclear Regulatory Commission, Washington, 1978.

[43] *Standard for probabilistic risk assessment for nuclear power plant applications,* ASME RA-Sa-2003, Addenda A to ASME-RA-S-2002, American Society of Mechanical Engineers, December 5, 2003.

[44] *Guide for incorporating human action reliability analysis for nuclear power generating stations,* IEEE Standard 1082, Institute of Electronic and Electrical Engineers, (1997/reaffirmed, 2001).

[45] *Good practices for implementing human reliability analysis*, NUREG-1792, US Nuclear Regulatory Commission, Washington, D.C., 2005.

[46] Swain, A.D. *Comparative Evaluation of Methods for Human Reliability Analysis.* Gesellschaft fur Reaktorsicherheit (GRS), GRS-71, Koln Germany, ISBN 3-923875-21-5, 1989.

[47] *Evaluation of human reliability analysis methods against good practices*, NUREG-1842, Draft for Public Comment, US Nuclear Regulatory Commission, Washington, D.C., April 2006.

[48] Dougherty, E.M. Guest editorial: human reliability analysis–where shouldst thou turn*? Reliability Engineering & System Safety, 29*: 281-299, 1990.

[49] *Probabilistic Risk Assessment Reference Document*, NUREG-1050, U.S. Nuclear Regulatory Commission, Washington, DC, 1984.

[50] Bieder, C., Le-Bot, P., Desmares, E., Bonnet, J-L., Cara, F. "MERMOS: EDF's new advanced HRA method," in *Probabilistic Safety Assessment and Management (PSAM 4),* A. Mosleh and R.A. Bari (Eds), Springer-Verlag, New York, 1998.

[51] Potash, L.M. et al. *Experience in integrating the operator contributions in the PRA of actual operating plants.* ANS/ENS Topical Meeting on PRA, Port Chester, NY. LaGrange, IL: American Nuclear Society, 1981.

[52] Phillips, L.D, Humphreys, P.C., and Embrey, D.E. *A Sociological Approach to assessing Human Reliability,* Oak Ridge, TN, Oak Ridge National Laboratory, 83-4, 1983.

[53] Embrey, D.E. *The use of performance shaping factors and quantified expert judgment in the evaluation of human reliability: an initial appraisal,* NUREG/CR-2986, Brookhaven National Laboratory, Upton, NY, 1983.

[54] Hannaman, G.W., Spurgin, A.J., and Lukic, Y.D. A model for assessing human cognitive reliability in PRA studies. In: *Proceedings of 1985 IEEE third conference on human factors and power plants, Monterey, California*, 85CH22350, IEEE, New York,1985.

[55] Embrey, D.E., Humphreys, P., Rosa, E.A., Kirwan, B., and Rea, K. *SLIM-MAUD: An approach to assessing human error probabilities using structured expert judgment (Vols. I & II),* NUREG/CR-3518, Brookhaven National Laboratory, Upton, NY, 1984.

[56] Hannaman, G.W., and Spurgin, A.J. *Systematic human action reliability procedure.* Electric Power Research Institute, EPRI NP-3583, 1984.

[57] Wakefield, D.J., Parry, G.W., Hannaman, G.W., and Spurgin, A.J. *SHARP1 - A revised systematic human action reliability procedure,* EPRI TR-101711, Tier 2, Electric Power Research Institute, December 1992.

[58] Swain, A.D. *Accident sequence evaluation program human reliability analysis procedure,* NUREG/CR-4772, SAND86-1996, Sandia National Laboratories, February 1987.

[59] Whitehead, D. W. *Recovery actions in PRA for the Risk Methods Integration and Evaluation Program (RMIEP), Volume 2: Application of the Data-Based Method,* NUREG/CR-4834, *Vol. 2*, U.S. Nuclear Regulatory Commission, Washington, DC, 1987.

[60] Williams, J.C. A Data-based method for assessing and reducing human error to improve operational performance, In: *Proceedings of IEEE Fourth Conference on Human Factors and Power Plants*, New York, IEEE, 1988.

[61] Spurgin, A.J., et al. *Operator reliability experiments using power plant simulators,* Electric Power Research Institute (EPRI), EPRI NP-6937, Vol. 1, 1990.

[62] Gertman, D.I., Blackman, H.S., Haney, L.N., Seidler, K.S., and Hahn, H.A. INTENT: A method for estimating human error probabilities for decision based errors. *Reliability Engineering & System Safety*, 35: 127-136, 1992.

[63] Parry, G., et al. *An approach to the analysis of operator actions in PRA*, Electric Power Research Institute (EPRI), EPRI TR-100259, 1992.

[64] Cacciabue, P.C., et al. *COSIMO: A cognitive simulation model of human decision making and behavior in accident management of complex plants,* IEEE Transactions on Systems, Man, and Cybernetics, *22(5)*, 1058 - 1074, 1992.

[65] Bareith, A., Hollo, E., Borbely, S., and Spurgin, A.J. Treatment of human factors for safety improvements at the Paks Nuclear Power Plant, In*: Probabilistic Safety Assessment & Management '96: ESREL '96 - PSAM-III*, Cacciabue, P.C., and Papazoglou, I. A. (Eds), Springer-Verlag, Berlin, 1996.

[66] Gertman, D.I., Blackman, HS, Byers, J., Haney, L., Smith, C., and Marble, J. "The SPAR-H Method," NUREG/CR-6883, U.S. Nuclear Regulatory Commission, Washington, DC, August 2005.

[67] Hallbert, B., Gertman, D., Lois, E., Marble, J., Blackman, H., and Beyers, J. The use of empirical data sources in HRA, *Reliability Engineering & System Safety*, 83: 139-143, 2004.

Distribution

5	MS 0748	J.A. Forester, 06761 (5 paper copies)
1	MS 0899	Technical Library, 9536 (electronic copy)


Sandia National Laboratories