Task Decomposition in Human Reliability Analysis

Ronald L. Boring* **and Jeffrey C. Joe**
Idaho National Laboratory, Idaho Falls, Idaho, USA

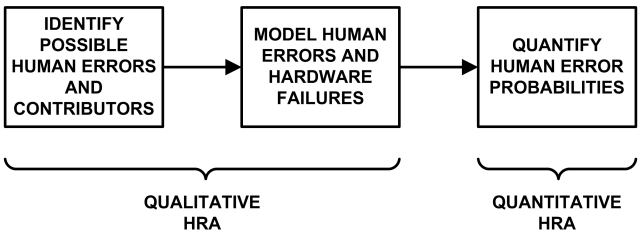
Abstract: In the probabilistic safety assessments (PSAs) used in the nuclear industry, human failure events (HFEs) are determined as a subset of hardware failures, namely those hardware failures that could be triggered by human action or inaction. This approach is top-down, starting with hardware faults and deducing human contributions to those faults. Elsewhere, more traditionally human factors driven approaches would tend to look at opportunities for human errors first in a task analysis and then identify which of those errors is risk significant. The intersection of top-down and bottom-up approaches to defining HFEs has not been carefully studied. Ideally, both approaches should arrive at the same set of HFEs. This question remains central as human reliability analysis (HRA) methods are generalized to new domains like oil and gas. The HFEs used in nuclear PSAs tend to be top-down—defined as a subset of the PSA—whereas the HFEs used in petroleum quantitative risk assessments (QRAs) are more likely to be bottom-up—derived from a task analysis conducted by human factors experts. The marriage of these approaches is necessary in order to ensure that HRA methods developed for top-down HFEs are also sufficient for bottom-up applications.

Keywords: HRA, human failure events, task decomposition, error of commission, latent error.

1. INTRODUCTION

Human reliability analysis (HRA) is a systematic approach to identify sources of human error and quantify their likelihood. As depicted in Boring (2009), at a high level, HRA may be seen as having three distinct phases (see Figure 1). The first phase is to identify possible human errors and their contributors. The second phase is to determine how these errors may be modelled in terms of an overall risk model such as a probabilistic safety assessment (PSA), which includes the interplay of hardware failures and human errors. Finally, these sources of human error are quantified to produce a human error probability (HEP) and accompanying uncertainty bounds. In practice, identifying and modelling may be considered qualitative aspects of HRA, while the final phase is associated with quantification.

Figure 1: Three General Phases of Human Reliability Analysis (Boring, 2009).



Different HRA methods have been developed to address these three phases, and some methods focus primarily on individual phases. Surprisingly, the area that remains least addressed across various HRA methods is the middle phase—modeling. This paper summarizes available guidance on modeling in HRA in support of oil and gas applications. As HRA is refined and subsequently more fully

* Ronald.Boring@inl.gov

incorporated into the safety and risk analyses performed in the oil and gas industry, it is imperative that all phases of HRA are thoroughly addressed.

HRA methods do not have a consistent level of task decomposition at the modeling phase. This lack of consistency can result not only in different qualitative analyses but also different HEPs. The level of task decomposition affects the dependency between tasks, which may have a further effect in driving the HEP. The issue is not that different HRA methods necessarily produce different results for the same HFE; rather, different HRA methods may decompose the HFE to different levels. Thus, the quantification of the same HFE may entail different assumptions and, to some extent, different groupings of tasks across HRA methods. In other words, because of a lack of a common task decomposition framework, HRA methods may not be using the same unit of analysis when producing the HEP.

For example, the European *Human Factors Reliability Benchmark Exercise* (Poucet, 1989), also referred to as the "Ispra Study" within the HRA community, demonstrates how central this topic is to HRA. The benchmark featured three phases of analysis to compare HRA methods. Each successive phase served to further bound the level of decomposition that defined the HFE. The first phase included identification of HFEs and their quantification by different analysis teams. Because different HFEs were identified across methods, it was difficult to compare method results directly. The second phase involved a more explicit definition of the HFEs to ensure the analysis teams quantified the same HFE. Even with a commonly defined HFE, there was considerable variability in how analysis teams modeled the HFE. Differences in task decomposition played a significant role in the differences of the HEPs for the HFEs. Some analysis teams decomposed to a finer level, resulting in lower HEPs. However, the dependencies between HFEs were not well accounted for in the analyses with finer grained task decomposition, resulting in unrealistically low HEP values in the authors' opinion. As such, a third phase was conducted, this time with an explicit decomposition of tasks and a common HRA event tree used in quantification.

The purpose of this paper is to review existing guidance on modeling human error in HRA and synthesize the disparate guidance into a simple framework that can be used in support of HRA in petroleum applications. The goal of establishing a common framework for human error modeling is to eliminate potential sources of variability in HEP quantification across methods. This paper presents initial insights derived from a literature review of applicable sources. Additional guidance will be developed and reported in the future.

2. DEFINING HUMAN ERROR

2.1 Human Error and Human Failure Events

HRA depicts a cause and effect relationship of human error. The *causes* are typically catalogued in terms of qualitative contributions to a human error, including the processes that shaped that error and the failure mechanisms. The processes—cognitive, environmental, or situational—that affect human error are typically referred to as performance shaping factors (PSFs). The resultant *effect* is the manifestation of human error—often called the failure mode. This failure mode is treated quantitatively and has an associated failure probability, the HEP.

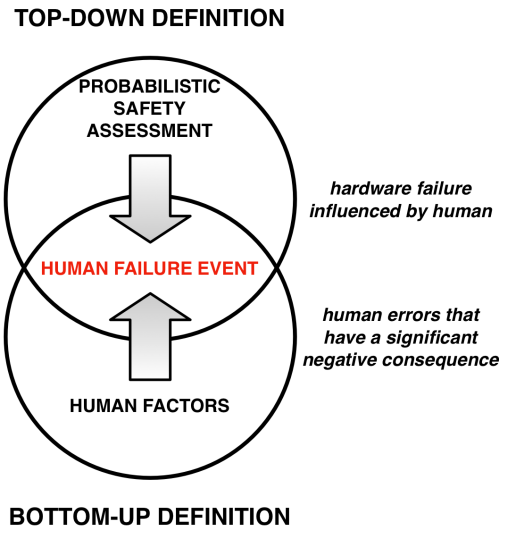
The term *human error* is often considered pejorative, as in suggesting that the human is in him- or herself the cause of the failure mode (Dekker, 2006). This belies the current accepted understanding that human error is the product of the context in which the human operates. In other words, it is not the human as the ultimate cause of the error but rather the failure mechanisms that put the human in a situation in which the error is likely to occur. The colloquial term, human error, is further challenged in that a human error may manifest but have little or no risk consequence. Human errors may be recovered or may simply not have a direct effect on event outcomes. Such risk insignificant occurrences are typically screened out of the HRA model.

Thus, to denote a risk significant human error, the term *human failure event* (HFE) has been posited. According to the American Society of Mechanical Engineers (ASME), a human failure event is "a basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or an inappropriate action" (2009). The HFE is therefore the basic unit of analysis used in PSA to account for HRA. While an HFE may be incorporated as a simple node in a fault tree or a branch in an event tree, the documentation supporting the HFE represents an auditable holding house for qualitative insights used during the quantification process. These insights may be simple to detailed, depending on the analysis needs and the level of task decomposition.

In PSAs used in the nuclear industry, as per the ASME definition, HFEs are determined as a subset of hardware failures, namely those hardware failures that could be triggered by human action or inaction. This approach is top-down, starting with hardware faults and deducing human contributions to those faults. Elsewhere, there is a bottom-up approach. More traditionally human factors driven approaches would tend to look at opportunities for human errors first in a task analysis and then model them in terms of potential for affecting safety outcomes. The order of identifying vs. modeling HFEs as shown in Figure 1 may be seen as changing depending on the approach. A top-down approach would tend to model the opportunity for HFEs and only then identify the sources of human error. In contrast, a bottom-up approach would first identify sources of human error and then model them in the PSA.

The intersection of top-down and bottom-up approaches to defining HFEs has not been carefully studied. Ideally, both approaches should arrive at the same set of HFEs. This question is crucial, however, because the HFEs used in nuclear PSAs tend to be top-down—defined as a subset of the PSA hardware faults—whereas the HFEs used in petroleum QRAs are more likely to be bottom-up—derived from a task analysis conducted by human factors experts. The marriage of these approaches is necessary in order to ensure that HRA methods developed for top-down HFEs are also sufficient for bottom-up applications. Figure 2 depicts the top-down and bottom-up approaches to defining HFEs. As can be seen, it is possible that both approaches arrive at the same solution. However, the solution set for the top-down and bottom-up approaches should be seen in terms of two circles in a Venn diagram. The problem is not that the HFEs may indeed overlap; the problem is that these HFEs may not always be identical.

Figure 2: Two approaches to defining human failure events.



Additionally, some HFEs used in a petroleum context are derived from barrier analysis and are prospective in nature, designed to identify how the defense in depth of a system may be increased to ensure the safety of a system to be built. This approach may emphasize the evolving timescale of

barrier effectiveness, whereas most conventional PSAs represent a static snapshot of an HFE. The barrier analysis approach is rarely used in contemporary PSAs for the nuclear industry. Additional guidance will be necessary to link the human factors processes for identifying vulnerabilities with the PSA fault modeling in HRA (Boring and Bye, 2008).

2.2 Limitations of the Top-Down Approach

As depicted in Figure 2, there are areas covered in the bottom-up approach that are not necessarily covered by the top-down approach (and vice versa). In this section, we discuss two noted shortcomings of the traditional top-down approach to defining HFEs—namely, errors of commission and latent errors, neither of which is adequately accounted for in traditional PSAs. We argue that the bottom-up approach provides better opportunity to incorporate these commonly omitted types of human error.

As noted, the top-down approach to defining HFEs begins by modeling those hardware systems that can fail and whose failure can be influenced by human actions or inactions. For example, if a particular electrical bus is a risk significant vulnerability to the overall system safety, the risk analyst would identify the failure of the bus as the starting point. He or she would next determine if the system is controlled by human operators. If yes, and if the human action is a significant subset of the overall risk of the bus failure, an HFE is modeled. The risk analyst must then determine what types of human errors are possible. This is often accomplished by referencing operating procedures and identifying which steps could be performed incorrectly. It is easier to identify a failure to execute particular required procedural steps than it is to postulate all the possible deviation paths the operator could follow that aren't encompassed by the procedure. In other words, the steps omitted (i.e., errors of omission) are more readily modeled than extra steps performed beyond the procedures (i.e., errors of commission). Thus, the top-down approach has exhibited far greater success in including relevant errors of omission than in anticipating possible errors of commission.

Already in one of the key early HRA textbooks, Gertman and Blackman (1994) elaborated on how the HRA methods of that time did not account for errors of commission very well, particularly ones that are more cognitive in nature. That is, while the earliest HRA method, THERP (Swain & Guttmann, 1983), provided failure rates for manual control actions (e.g., simple, skill-based tasks which can include errors of commission that can be quantified), there was and is still no widely accepted approach that can account for errors of commission that fall outside of slips and lapses (and the PSFs that influence these error types). To model errors of commission that are more cognitively based (i.e., not skill-based manual control actions), Gertman and Blackman state that the practice at that time was to quantify errors of commission using simplified commission models (e.g., selection errors), or to use screening values to estimate a crew's probability of successfully diagnosing an event (e.g., SHARP – Hannaman & Spurgin, 1984; ASEP – Swain, 1987). Yet, we find that these methods still do not provide enough specific and useful guidance to help come up with an actionable approach to bridge this gap between the top-down and bottom up approaches.

Straeter, Dang, Kaufer, and Daniels (2004) argued that first generation HRA methods were not effective in characterizing, predicting, and preventing accidents such as Three Mile Island, which featured significant errors of commission. They argued further that this failure was because first generation methods did not have the necessary human performance data, a way of representing errors of commission that are not simple, skill-based manual control actions, nor a methodological framework designed to handle these kinds of errors of commission. Second generation methods were developed in part to address these shortcomings in first generation methods, but somewhat ironically, there was also increased pressure to have these second generation methods be less labor intensive in their methodology, which often meant that some of the more time consuming aspects of HRA were truncated or eliminated altogether (e.g., no explicit guidance in many newer methods on how to define HFEs). The result is that many second generation HRA methods still struggle with how to handle errors of commission that are more cognitively based.

Work by Reer, Dang, and Hirschberg (2004); Reer and Dang (2007); and Podofillini and Dang (2012) on the Commission Errors Search and Assessment (CESA) method has been an important and proactive step in helping address a part of this errors of commission issue in HRA. These researchers have developed CESA as a systematic approach to, "Identify potentially risk-significant EOCs [errors of commission], given an existing PSA [probabilistic safety analysis]." (Reer, Dang, & Hirschberg, 2004; pg. 189). One point that these researchers emphasize is that, given their focus on identifying errors of commission that are easier to quantify, CESA provides a straightforward and streamlined approach to determining which errors of commission are important to consider in PSA. Specifically, CESA focuses on *active* errors of commission that operators make while following control room procedures, rather on the more nebulous *latent* errors of commission managers and designers could make in decision-making, which are often more difficult to quantify because they are determined by multiple distal factors that are further influenced by transient contextual circumstances.

We believe there is an important distinction to make between *active* errors of commission and *latent* errors of commission. Reason (1990) defines active and latent errors as follows:

> In considering the human contribution to systems disasters, it is important to distinguish two kinds of error: active errors, whose effects are felt almost immediately, and latent errors, whose adverse consequences may lie dormant within a system for a along time, only becoming evident when they combine with other factors to breach the system's defences….In general, active errors are associated with the performance of 'front-line' operators of a complex system: pilots, air traffic controllers, ships' officers, control room crews and the like. Latent errors, on the other hand, are most likely to be spawned by those whose activities are removed in both time and space from the direct control interface: designers, high-level decision makers, construction workers, managers and maintenance personnel. (pg. 173)

Woods, Johannesen, Cook, and Sarter (1994) and Hollnagel (1998) also identified this very strong correlation between active errors and errors that occur at the "sharp end" of the work production processes, and latent errors and errors occurring at the "blunt end" of the process. More importantly, with respect to this paper, Reason (1990) and others have repeatedly made the point that latent errors—both latent errors of commission and latent errors of omission—are more risk-significant than active errors.

The analysis of significant operating events at commercial nuclear power plants (e.g., NUREG/CR-6753, 2001) further supports the conclusions of Reason (1990), Gertman and Blackman (1994), and Woods, Johannesen, Cook, and Sarter (1994). NUREG/CR-6753 used data from the U.S. Nuclear Regulatory Commission's (NRC) Accident Sequence Precursor (ASP) Program and the Human Performance Events Database (HPED) to identify safety significant events in which human performance contributed to changes in risk. The sensitivity analyses performed using these data showed that human performance contributed significantly to analyzed events. In particular, two hundred and seventy human errors were identified in the events reviewed, and multiple human errors were involved in every event. More importantly, latent errors (i.e., failures to correct known problems and errors committed during design and maintenance activities) were present four times more often than were active errors. These results confirm the assertion that latent errors contribute significantly to risk-significant events.

The *Deepwater Horizon* accident is one notable example from the petrochemical industry on how a top-down approach to identifying HFEs can miss important human errors. We analyzed this event in greater detail for this paper for two reasons. First, it is an event that occurred in the petrochemical industry, and therefore has more relevance for this paper than other events that have occurred in the nuclear industry and elsewhere (e.g., transportation). Second, other significant events, such as Three Mile Island and Chernobyl have been analyzed extensively relative to the *Deepwater Horizon* accident.

While there were many contributing factors that were responsible for the *Deepwater Horizon* accident, analyses of the events leading up to the accident clearly show that latent errors of commission played a

significant role. That is, while multiple safety systems on the *Deepwater Horizon* offshore oil-drilling rig actively failed on 20 April 2010, they failed in large part because of latent errors of commission. There were numerous errors in human decision making whereby information on the system's state that were leading indicators of impending problems were misinterpreted, discounted, or ignored, and the decision to proceed with operations was made. These decision-making errors were at both the operations (i.e., tactical) and management (i.e., strategic) level, resulting in the largest oil spill in U.S. history.

With respect to operations related decision-making errors, the well that had been drilled into the Macondo Prospect oil field had a blowout preventer (BOP) on its wellhead, but according to various news reports and event investigation reports, operations continued even though there were components on the BOP that were known to be damaged. Namely, the annular (i.e., a rubber donut-shaped gasket that closes around the drilling pipe to seal the well) and the control pods, which contain the instrumentation and control systems for the BOP, were damaged and/or not fully functional prior to the event. In the case of the annular, it had become "stripped" a month before the accident. That is, it was intentionally closed around the pipe, and the pipe was moved up and down to strip over 40 joint tools attached to it. When the stripping was completed, according to the Deepwater Horizon Study Group (2011) report, witnesses reported seeing pieces of rubber in the drilling fluid that had risen to the top of the well. According to the National Research Council (2011) report, the annular was apparently, "Untested for integrity afterwards. Annulars are often unable to seal properly after stripping" (pg. 52). With respect to the control pods, there was a primary and backup control pod installed on the BOP, but according to the American television newsmagazine program, *60 minutes* (CBS News, 2011), management and operations were aware that one of the control pods was not fully functional, meaning there were known potential issues with its reliability if it were to be called upon to actuate important safety functions in the event of an emergency.

With respect to management related decision-making errors, according to Bronstein and Drash (2010), on the day *Deepwater Horizon* event occurred, drilling operations were behind schedule by approximately five weeks. To hasten progress in finishing the well, as three concrete plugs were being placed in the column of the well, management from British Petroleum decided to use seawater to keep the pressure from the oil well under control instead of "drilling mud." Others, including the drilling rig's chief driller, challenged this decision. It was also reported by Bronstein and Drash that workers on the oil drilling platform had a tacit understanding that they could get fired or face other chilling effects for bringing up safety concerns that would delay progress on drilling operations, implying that there were problems with the organization's safety culture.

Clearly, there were both tactical and strategic errors of commission that contributed to the *Deepwater Horizon* accident. Whittingham (2004) presents another way of characterizing errors of commission that differs from the tactical and strategic delineation used above. Whittingham proposed that errors of commission with significant cognitive aspects often have errors: 1) at the organizational and management level, 2) in the design, and 3) in maintenance activities. Using Whittingham's characterization scheme reveals additional insights into the nature of the errors of commission committed prior to this event.

Namely, there were organizational and management errors in that management made decisions to put profit over safety. Design errors also contributed to this event in that the BOP did not have a well designed component called the blind shear ram (BSR). The BSR is made up of two metal blades on opposing sides of the pipe in the bore hole that are designed to come together in a scissor like motion to cut the pipe, effectively preventing the well from leaking. According to the National Academy of Engineering's final report (2011), the BSR on Deepwater Horizon's BOP had a known design flaw that would affect its ability to perform its designed safety function. In particular, engineering analyses of the BSR prior to the accident had documented the fact that it would have trouble shearing a pressurized pipe, particularly if the pipe was not perfectly aligned with cutting surfaces of the BSR.

As previously discussed, maintenance errors also contributed to this event in that the control pods on the BOP were known to be not fully functional prior to the accident and that the annular had experienced stripping in the month preceding the accident, and yet drilling operations were not halted to repair these safety systems.

The point of this more detailed analysis of the *Deepwater Horizon* accident is to show the ways in which latent errors of commission, and in particular errors of commission related to decision-making and other cognitively intensive activities, can lead to catastrophe. Furthermore, it is not apparent that a traditional top down approach, whereby active errors at the sharp end derived from the identification of the most risk significant hardware failures are converted into HFEs, would have identified these tactical, strategic, organizational, design, and maintenance errors that occurred at the blunt end of the work processes. Either the top down approach needs to identify how HFEs based on latent errors can credibly affect system safety, or additional analyses using other approaches need to be included so that these blunt end errors can be identified and converted into meaningful HFEs that can be effectively incorporated into QRA.

3. EXISTING METHOD GUIDANCE ON MODELING HUMAN FAILURE EVENTS

Switching directions now, in this section we briefly review a number of available methods, guidance documents, and standards for HRA to derive potential rules for decomposing tasks to define HFEs. The methods review is centered on U.S. approaches, since these have been the sources widely used by analysts and documented in nuclear applications. Additional insights may be derived by careful study of non-U.S. HRA methods.

3.1 U.S. HRA Methods

THERP. The task analysis model in the Technique for Human Error Rate Prediction (THERP) is described in Chapter 4 of NUREG/CR-1278 (Swain and Guttman, 1983). It uses a goal-task breakdown of human activities to answer what are the goals of the human in terms of their interface with equipment such as controls. Task analysis classifies human activities into dynamic (involving interpretation and decision-making) and step-by-step (continuous or on-going) tasks. These tasks are included in the HRA event trees as branches. Since the tasks are modeled at the level of each step in a sequence of actions, the task decomposition may be considered quite detailed. These subtasks can be combined to represent an overall human action, and THERP provides clear guidance on aggregating subtasks during quantification.

Importantly, THERP provides a dependency model—which calculates how the relationship between subtasks should be treated in mathematical terms when aggregating the HEP. In other words, related tasks should not be double-counted when computing the likelihood of error. The dependency model in THERP has been adopted by almost every subsequent HRA model. The contemporary application of dependency is, however, considerably different from the original use in THERP (Whaley et al., 2012). In the original THERP application, dependency was used to account for subtasks that were closely related, typically in terms of using the same crew, occurring close in time, with little new contextual information. Dependency in THERP modeled intra-task relations, not inter-task relations. In fact, the point at which no relationship between tasks existed was considered the point at which the task was fully defined and constituted a complete HFE. Ironically, current use of dependency is almost exclusively for inter-task relations *between* HFEs. This is a widespread misapplication of the original THERP guidance and has the potential to result in different HFEs.

ASEP. The Accident Sequence Evaluation Process (ASEP) method (Swain, 1987) came about as a simplification of THERP. It does not include a unique process to model HFEs but instead defers to THERP and to PSA judgment about relevant tasks to analyzed. In contrast to THERP, there is a stronger emphasis on the need not to analyze every task, particularly for screening analyses. Thus, the clear definition for an HFE provided in THERP was loosened by the time ASEP was released.

SPAR-H. The Standard Plant Analysis Risk-Human Reliability Analysis (SPAR-H) method (Gertman et al., 2005) is a simplified HRA approach based in part on THERP (Boring and Blackman, 2007). SPAR-H provides no explicit guidance on task decomposition or defining or modeling the HFE beyond considering action and diagnosis tasks separately. SPAR-H defers to the IEEE 1082 and ASME PSA standards (discussed below) for discussion on how to model HFEs (i.e., decompose the tasks) for inclusion in the PSA. SPAR-H assumes the HFE is predefined, and the method therefore does not devote extensive time to telling the analyst how to formulate the HFE.

ATHEANA. A Technique for Human Error Analysis (ATHEANA; US Nuclear Regulatory Commission, 2000; see also Forester et al., 2007) provides nine overall steps, several of which are related to identifying HFEs. Using the ATHEANA approach, it is possible to determine if the modeled event should be considered an HFE or an unsafe action (UA). The delimiter is based on the consequence in terms of contribution to core damage—an UA is akin to a human error that is not risk significant. The ATHEANA method also provides guidance on determining errors of commission.

In practice, the final ATHEANA step—incorporation into PSA—is not as clearly articulated as the other steps, leading to some problems using ATHEANA to define HFEs. ATHEANA takes a holistic approach to HRA, and its task decomposition may be seen at the scenario or overall unsafe action level. ATHEANA considers unsafe acts, but the specific aggregation of these into the HFE remains underspecified. Importantly, ATHEANA considers deviations from nominal scenarios. These represent possibly unsafe conditions at the plant caused by operator action or inaction. The likelihood of these nominal scenarios is considered in the quantification of the overall HFE. Additional guidance (NUREG-1880) states that the human reliability analysts should work with the PSA team to model the HFE consistent with the PSA. This latter guidance points to a lack of clear guidance on modeling the HFE at a level consistent with the PSA. Since the SPAR-H method (Gertman et al., 2005) points analysts to the ATHEANA method specifically to identify and model human errors as needed, there is a troubling disconnect between both ATHEANA and SPAR-H and the practicable HFE in a PSA.

CBDT. The Cause-Based Decision Tree (CBDT) method (EPRI, 1992), widely used in industry, uses a decision tree approach to arrive at the quantification of HFEs based on key pieces of information (decision points) about operator performance. The method uses the SHARP1 framework for task decomposition as described in the next section.

3.2 Standards and Guidance Documents in HRA

SHARP1. The Systematic Human Action Reliability Procedure Revision 1 (SHARP1; EPRI, 1992) is an extension of the original SHARP process used for integrating HRA into the PSA process. The first stage of the SHARP1 process is the identification of the HFEs that are quantified in a subsequent stage. This first stage outlines five steps to arrive at the HFE:

1. Define the human interactions with the system that are potentially of interest. These are typically those that could leave some part or function of the plant unavailable. The procedure recommends identifying both errors of omission and commission as they might impact the plant.
2. Screen these human interactions to reduce the scope of the analysis to those that are most important.
3. Break down subtasks according to procedures to identify those subtasks that may have an impact on the plant. The emphasis here is to identify any tasks that may leave specific parts or functions of the plant unavailable, even if only temporarily as part of routine plant operations.
4. Perform an impact assessment to determine what effect the human subtasks have on plant equipment and plant state.
5. Integrate the human interactions as HFEs into the plant PSA model.

The approach falls short at defining an adequate way to decompose the overall event in terms of analysis. For example, if applying the five steps, particularly Step 3, it would not be clear whether to use a method to quantify the subtasks, groupings of subtasks, or the overall human interaction with the

system, which could encompass hundreds of subtasks. This lack of decomposition can result in a myriad of HEPs, as many methods are not sensitive to subtask vs. task level analysis.

IEEE-1082 (1997). This standard, currently under revision, advocates a "stepwise" incorporation of human actions into the PSA model. The process begins with a complete but not unnecessarily detailed inclusion of human actions. These actions are considered in terms of risk-significance, such that only human actions that truly drive core damage frequency should be considered. A screening analysis narrows the number of human actions that are considered in the PSA. Some actions may be revisited at a later time when additional detail is added to the PSA model. The HFEs that are risk significant are modeled in sufficient detail to allow quantification. The IEEE-1082 standard is a very high level document. As such, it better addresses screening human errors for risk significance than actually defining those errors as HFEs.

ASME/ANS RA-Sa (2009 Revision). The ASME PSA standard explicates a number of important points to consider in HRA but does not provide specific recommendations on modeling HFEs beyond providing a formal definition of HFEs (see Section 2.1). The standard requires documentation of the identification, characterization, and quantification of pre-initiator, post-initiator, and recovery human actions, but it does not advocate a particular approach or recommend the appropriate level of decomposition. According to the standard, HFEs must be defined and included for each human activity that is not screened out and must be defined to reflect the resulting unavailability of a component, train, system, or function that is modeled in the PSA. The standard does provide guidance that several human activities may be grouped into a single HFE if the impact of the activities is similar. Three levels of HFEs are defined, differentiated by those HFEs that do not perform a task analysis, those that have a high-level task analysis (e.g., human impact at the train level), and those that have a detailed task analysis (e.g., human impact on individual components).

Good Practices for HRA (NUREG-1792). As with the standards mentioned above, the *Good Practices* link the HFE to the specific hardware failure that results from the human action or inaction. The level of modeling (i.e., level of decomposition) should reflect the amount of plant hardware that is affected. Thus, the HFE may be defined at the component, train, system, or function level. Human actions may be grouped at a higher level as appropriate. For example, if multiple human actions affect multiple components in the train, the HFE should be modeled at the train level. If, however, quantification differs considerably between the component and train level of modeling, the more conservatively bounding HFE definition should be used. If grouping multiple actions masks the potential for considering subsequent dependencies, the actions should be modeled as individual HFEs. This guidance is helpful in establishing the boundaries between HFEs in an event evolution, although it fundamentally reflects the top-down definition of the HFE.

3.3 Other Considerations

Dynamic modeling. In developing human performance simulation models, the issue of task decomposition resurfaces. Simulation models like ADS-IDAC (Chang and Mosleh, 2007) feature the ability to model human performance at the very detailed subtask level, such as decision points and simple manual actions. While quantification is possible at the subtask level, the models do not provide guidance for combining subtask HEPs into the HFE level appropriate for a PSA. Such combinatorial quantification must consider dependencies between subtasks, but there is the possibility to inflate HEP values if the aggregation algorithm does not properly consider the small subtasks that the simulation models use (Boring, 2007). Additionally, dynamic modeling reveals the need for PSF latency—namely, that PSFs must not be considered discretely without the lingering effect from one time point to another. For example, stress cannot simply be turned off because the underlying cause of that stress has disappeared. This insight suggests that PSFs may need to play a role in defining the HFEs, or at least the boundaries between HFEs.

HERA/SACADA. The Human Event Repository and Analysis (HERA) database system (Hallbert et al., 2006) and its descendent, the Scenario Authoring, Characterization, and Debriefing Application

(SACADA) database (Chang et al., in press), provides guidance on how to decompose events into subevents suitable for a detailed understanding of human performance. An event may be any human action or inaction that negatively affects plant safety. A human-related event may be further broken into subevents, according to the following criteria:

- Are separate people involved across the span of the event?
- Does an action within the event have a different goal than other actions?
- Does an action involve different equipment?
- Does an action have different consequences than the overall event being modeled?

HERA and SACADA subevents may be identical to HFEs in an HRA or PSA, but they are often more detailed in nature, because the purpose of the database system is to capture as much information as possible about human performance. As such, these subevents are not screened in terms of risk significance the way HFEs are in the HRA and PSA. Still, the fundamental guidance provided on decomposing events is useful in defining HFEs, and it provides a more bottom-up approach than is typical.

4. CONCLUSIONS

Defining an HFE for use in novel HRA applications still remains somewhat elusive. Although general guidance exists for the top-down approach, there remains a large element of skill of the craft in actually decomposing groups of subtasks into an HFE suitable for inclusion in the PSA. While approaches exist for bottom-up definitions, these still do not adequately address topics such as latent errors or errors of commission. Nonetheless, several candidate principles of HFE modeling have emerged from our review in this paper:

- Until clear guidance is available to identify commonalities and differences between the top-down and bottom-up approaches, it is desirable to employ a combination of both approaches to define the HFE.
- When adopting the top-down approach, the definition of the HFE should start broad, identifying those human actions and inactions that may trigger the unavailability of components, systems, or functions.
- These broad HFEs should be screened to determine the risk significant activities. The risk significant activities are the primary HFEs that are modeled in greater detail in the HRA.
- Task analysis of these risk significant activities may reveal additional sources of failures that may not be anticipated in the initial definition of the HFE. This represents the bottom-up approach. The definition of the HFE and screening should be an iterative process to arrive at a complete and relevant model of the human contribution to the overall system risk.
- Bottom-up approaches should consider errors of commission and latent errors in crafting the HFEs.
- Subtasks may reasonably be grouped into a single HFE provided that they are logically related; they do not represent different tasks, personnel, or equipment; and they do not mask dependencies that need to be accounted for.
- The earliest HRA methods used a simple equipment-level task decomposition. This is the level of flipping a switch. As interfaces have progressed in complexity, the interaction of the human with the equipment may represent a much higher level of decomposition that includes more cognitive or diagnostic activities. It is insufficient to define HFEs in terms of simple tasks—it must include a significant cognitive component as well.

These principles will be refined and developed into comprehensive guidance for defining HFEs in the petroleum context. Ultimately, one key goal of is to bridge the gap in existing HRA guidance and application to the petroleum domain. Current practice follows a somewhat vague top-down approach of using predefined HFEs from the PSA. As HRA is refined for oil and gas applications, it will need to include a clear bottom-up approach compatible with QRA.

Disclaimer

INL is a multi-program laboratory operated by Battelle Energy Alliance LLC, for the United States Department of Energy under Contract DE-AC07-05ID14517. This work has been carried out as part of The Research Council of Norway project number 220824/E30 "Analysis of human actions as barriers in major accidents in the petroleum industry, applicability of human reliability analysis methods (Petro-HRA)". Financial and other support from The Research Council of Norway, Statoil ASA and DNV are gratefully acknowledged. This paper represents the opinion of the authors, and does not necessarily reflect any position or policy of the above mentioned organizations. Neither the United States Government, nor any agency thereof, nor any of their employees makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately-owned rights.

References

American Society of Mechanical Engineers. (2009). Addenda to ASME/ANS RA-S–2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, ASME/ANS RA-Sa-2009. New York: American Society of Mechanical Engineers.

Boring, R.L. (2007). Dynamic human reliability analysis: Benefits and challenges of simulating human performance. In T. Aven & J.E. Vinnem (Eds.), *Risk, Reliability and Societal Safety, Volume 2: Thematic Topics. Proceedings of the European Safety and Reliability Conference (ESREL 2007)* (pp. 1043-1049). London: Taylor & Francis.

Boring, R.L. (2009). Human reliability analysis in cognitive engineering. *Frontiers of Engineering: Reports on Leading-Edge Engineering from the 2008 Symposium* (pp. 103-110). Washington, DC: National Academy of Engineering.

Boring, R.L., & Bye, A. (2008). Bridging human factors and human reliability analysis. *Proceedings of the 52nd Annual Meeting of the Human Factors and Ergonomics Society*, 733-737.

Bronstein, S. & Drash, W. (2010, June 9). Rig survivors: BP ordered shortcut on day of blast. Available from: http://www.cnn.com/2010/US/06/08/oil.rig.warning.signs/index.html

CBS News (2010, May 16). Blowout: The Deepwater Horizon disaster [Television series episode]. *60 minutes*. New York, NY.

Center for Chemical Process Safety (CCPS) (2008). *Guidelines for hazard evaluation procedures (3rd Edition)*. American Institute of Chemical Engineering/AIChE, New York, NY.

Chang, Y.J., Bley, D., Criscione, L., Kirwan, B., Mosleh, A., Madary, T., Nowell, R., Richards, R., Roth, E.M., Sieben, S., and Zoulis, A. (In press). The SACADA database for human reliability and human performance. *Reliability Engineering and System Safety.*

Chang, Y.H.J., and Mosleh, A. (2007). Cognitive modeling and dynamic probabilistic simulation of operating crew response to complex system accidents, part 1: Overview of the IDAC model. *Reliability Engineering and System Safety, 92*, 997-1013.

Deepwater Horizon Study Group. (2011). *Final report on the investigation of the Macondo well blowout. Center for Catastrophic Risk Management*, University of California at Berkeley, Berkeley, CA.

Dekker, S. W. A. (2006). *The Field Guide to Understanding Human Error.* Aldershot, UK: Ashgate Publishing Co.

EPRI. (1992). *An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, TR-100259.* Palo Alto: Electric Power Research Institute.

EPRI. (1992). *SHARP1—A Revised Systematic Human Action Reliability Procedure, EPRI TR-101711.* Palo Alto: Electric Power Research Institute.

Forester, J., Kolaczkowski, A., Cooper, S., Bley, D., and Lois, E. (2007). *ATHEANA User's Guide, NUREG-1880.* Washington, DC: US Nuclear Regulatory Commission.

Gertman, D. I., & Blackman, H. S. (1994). Human reliability and safety analysis data handbook. John Wiley & Sons, New York, NY.

Gertman, D., Blackman, H., Marble, J., Byers, J., Smith, C., and O'Reilly, P. (2005). *The SPAR-H Human Reliability Analysis Method, NUREG/CR-6883*. Washington, DC: US Nuclear Regulatory Commission.

Gertman, D., Hallbert, B., Parrish, M., Sattison, M., Brownson, D., & Tortorelli, J. (2001). *Review of findings for human error contribution to risk in operating events, NUREG/CR-6753*. Washington, DC: US Nuclear Regulatory Commission.

Gertman, D., Hallbert, B., & Prawdzik, D. (2002). *Human performance characterization in the Reactor Oversight Process, NUREG/CR-6775*. Washington, DC: US Nuclear Regulatory Commission.

Hallbert, B., Boring, R., Gertman, D., Dudenhoeffer, D., Whaley, A., Marble, J., & Joe, J. (2006). *Human event repository and analysis (HERA) system, overview*, *NUREG/CR-6903, Volume 1*. Washington, DC: US Nuclear Regulatory Commission.

Hollnagel, E. (1998). *Cognitive reliability and error analysis method (CREAM)*. Oxford: Elsevier.

IEEE. (1997). *Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations, IEEE-1082*. New York: Institute of Electrical and Electronics Engineers.

Kolaczkowski, A., Forester, J., Lois, E., and Cooper, S. (2005). *Good Practices for Implementing Human Reliability Analysis, Final Report, NUREG-1792*. Washington, DC: US Nuclear Regulatory Commission.

National Research Council. (2011). Macondo Well Deepwater Horizon Blowout: Lessons for Improving Offshore Drilling Safety. Washington, DC: The National Academies Press.

Podofillini, L., & Dang, V. (2012). Progress on Errors of Commission: an Outlook Based on Plant-Specific Results. *Proceedings of the 11th International Conference on Probabilistic Safety Assessment and Management*, 16B-Th5-1, Helsinki, Finland.

Poucet, A. (1989). *Human Factors Reliability Benchmark Exercise, Synthesis Report, EUR 12222 EN*. Luxembourg: Office for Official Publications of the European Communities.

Reason, J. (1990). *Human Error*. Cambridge: Cambridge University Press.

Reer, B., & Dang, V. (2007). *The Commission Errors Search and Assessment (CESA) Method. PSI Report No. 07-03*. Baden, Switzerland: Paul Scherrer Institute.

Reer, B., Dang, V., & Hirschberg, S. (2004). The CESA Method and its Application in a Plant-Specific Pilot Study on Errors of Commission. *Reliability Engineering and System Safety, 83*(2), 187-205.

Straeter, O., Dang, V., Kaufer, B., & Daniels, A. (2004). On the way to assess errors of commission. *Reliability Engineering & System Safety*, *83*(2), 129-138.

Swain, A.D. (1987) *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772. Washington, DC: US Nuclear Regulatory Commission.

Swain, A.D., & Guttmann, H.E. (1983) *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, NUREG/CR-1278. Washington, DC: US Nuclear Regulatory Commission.

US Nuclear Regulatory Commission. (2000) *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)*, NUREG-1624, Rev. 1. Washington, DC: US Nuclear Regulatory Commission.

Whaley, A.M., Kelly, D.L., and Boring, R.L. (2012). Guidance on dependence assessment in SPAR-H. *Joint Probabilistic Safety Assessment and Management and European Safety and Reliability Conference*, 27-Mo4-4.

Woods, D., Johannesen, L., Cook, R., & Sarter, N. (1994). *Behind human error: Cognitive systems, computers and hindsight, CSERIAC SOAR 94-01*. Columbus: Ohio State University.