

## **Good Practices for Implementing Human Reliability Analysis (HRA)**

---

---

Date: April 6, 2004

Prepared by  
Alan Kolaczowski and John Forester

Sandia National Laboratories  
Albuquerque, NM 87185

USNRC Project Manager: Erasmia Lois

Prepared for  
Probabilistic Risk Analysis Branch  
Division of Risk Analysis and Applications  
Methods Group  
Office of Nuclear Regulatory Research  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555

Draft

# Table of Contents

1.	INTRODUCTION .....	3
1.1	Background .....	3
1.2	HRA in the Context of PRA .....	4
1.3	Purpose .....	5
2.	OVERVIEW OF GOOD PRACTICES FOR HRA .....	6
2.1	Scope of HRA Good Practices Guidance .....	6
2.2	HRA Good Practices and the State-of-the-Art in HRA .....	6
2.3	Summary and Organization of HRA Good Practices Guidance .....	6
3.	HRA TEAM FORMATION AND OVERALL GUIDANCE .....	8
4.	PRE-INITIATOR HRA .....	10
4.1	Identifying potential pre-initiator human failures .....	10
4.2	Screening those activities for which human failure events do not need to be modeled .....	13
4.3	Modeling specific human failure events (HFES) corresponding to the human failures .....	15
4.4	Quantifying the corresponding human error probabilities (HEPs) for the specific HFES .....	16
5.	POST-INITIATOR HRA .....	24
5.1	Identifying potential post-initiator human failures .....	24
5.2	Modeling specific human failure events (HFES) corresponding to the human failures .....	27
5.3	Quantifying the corresponding human error probabilities (HEPs) for the specific HFES .....	30
5.4	Adding recovery actions to the PRA .....	39
6.	HRA DOCUMENTATION .....	42
7.	ERRORS OF COMMISSION (EOCs) .....	43
8.	REFERENCES .....	45
	ACKNOWLEDGMENTS .....	46
APPENDIX A	Guidance on Consideration of Performance-Shaping Factors for Post-Initiator HFES .....	47

Draft

# Good Practices for Implementing Human Reliability Analysis (HRA)

## 1. INTRODUCTION

### 1.1 Background

In accordance with its policy statement <sup>1</sup> on the use of probabilistic risk assessment (PRA), during the last decade the NRC has been increasingly using PRA technology in “all regulatory matters to the extent supported by the state of the art in PRA methods and data.” Examples of risk informed initiatives are: undertaking risk-informed rulemaking activities such as risk-informing 10CFR Part 50<sup>2</sup>, generating a risk-informed framework for supporting licensee requests for changes to a plant’s licensing basis (Reg Guide 1.174),<sup>3</sup> risk-informing the reactor oversight process, performing risk studies (e.g., for steam generator tube rupture (SGTR), and fire events), and evaluating the significance of events. In addition, the NRC is using PRA in the development of an infrastructure to licence new reactors.

Given the increasing importance of the role of PRA in regulatory decision making, it is crucial that decision makers have confidence in the results produced by PRAs. To support this, the NRC has issued Regulatory Guide 1.200<sup>4</sup> that describes an acceptable approach for determining the technical adequacy of PRA results for risk informed activity. Reg Guide 1.200<sup>4</sup> reflects and endorses guidance provided by standards produced by societies and industry organizations. It currently addresses the American Society of Mechanical Engineers (ASME) Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications<sup>5</sup> which was developed for a full power, internal events (excluding fire) Level 1 PRA and a limited Level 2 PRA, and the Probabilistic Risk Assessment Peer Review Process Guidance (NEI-00-02).<sup>6</sup>

The level of detail provided in the ASME Standard<sup>5</sup> and NEI-00-02<sup>6</sup> is at a high level, addressing what to do, but not how to do it., Consequently, there may be several approaches to address certain analytical elements, which though they may meet the standards, may do so by making different assumptions and approximations, and, therefore, produce different results. This is particularly true of human reliability analysis (HRA) (see section 1.2 for a discussion of HRA). Therefore, the guidance provided by these documents is not sufficient to address the detailed HRA quality issues needed to be considered in regulatory decision making. For example, in section A.8, Modeling of Human Performance, in Standard Review Plan 19,<sup>7</sup> the NRC staff is required to determine if “the modeling of human performance is appropriate.” While the ASME Standard<sup>5</sup> and NEI-00-02<sup>6</sup> can address whether the HRA addresses the right issues, they do not give guidance on how they are addressed. Therefore, in order to support the review of human performance issues in the context of PRAs, the NRC is developing this guidance for performing and reviewing HRAs, as a document supporting Reg Guide 1.200<sup>4</sup>. The guidance is being developed in two phases. The first phase is the development of this “HRA Good Practices” document which has been prepared on the basis of the NRC experience and lessons learned from developing HRA methods (e.g., THERP,<sup>8</sup> SLIM,<sup>9</sup> and ATHEANA<sup>10</sup>), performing HRAs (e.g., NUREG-1150<sup>11</sup> studies, and reviewing HRAs (in particular the individual plant examinations [IPEs])). The second phase is a review and evaluation of existing HRA approaches for their capability to meet the good practices when employed to address different regulatory applications.

This volume describes the NRC staff views regarding good practices of an HRA as implemented within a broader PRA. The volume is written in the context of a risk assessment for commercial nuclear power plant (NPP) operations occurring nominally at full power. However, it is likely that many of the good practices will also be applicable to low power and shutdown operations. Similarly, the volume is purposely aimed for applications involving internal initiating events but should generally be appropriate for external initiating events. Additionally, elements of this volume may be of benefit in examining human actions related to nuclear materials and safeguard types of applications.

As with any evolving technology, both PRA and the implementation of HRA within the PRA framework are continuing to improve. Hence, what is good practice today may be somewhat inferior or outdated tomorrow. Much of what is in this volume will always constitute good practice; some of it may be subject to newer technology, methods, and tools. For this reason, this volume must be considered a snapshot of good practices in HRA circa 2004.

With the expectation that PRA will continue to be used in the commercial nuclear industry in assessing current operating risks, in estimating changes in risk as a result of temporary and permanent plant changes to existing plants, and as an adjunct to the design process of newer generation plants, it is important that HRA practitioners perform human reliability analyses in accordance with good practices and that reviewers recognize the implementation of good practices (or failure to do so) in these analyses.

## **1.2 HRA in the Context of PRA**

Human reliability analysis in the PRA context is that discipline that identifies and provides probabilities for the human failure events that can negatively impact normal or emergency plant operations. The human failure events modeled in PRAs that are associated with normal plant operation include: 1) events that leave equipment in an unrevealed, unavailable state, such as miscalibration of a level sensor, 2) those that induce an initiating event, such as a human-caused loss of feedwater (typically captured by the initiating event frequency), or 3) those modeled as human events contributing to an initiating event, such as a total loss of service water (e.g., failing to backup the start of service water train B upon loss of train A). The human failure events modeled in PRAs associated with emergency plant operation include events that, if not performed, do not allow the desired function to be achieved, such as failing to initiate feed and bleed. Quantification of the probabilities of the human failure events is based on plant and accident specific conditions, where applicable, including any dependencies among actions and conditions.

This volume provides HRA good practices that when implemented will result in determining the impacts of human actions as *realistically as necessary* in an assessment of risk. Note the emphasis on realistic as necessary rather than as realistic as possible. For example, depending on the purpose for which the PRA is to be used, a conservative treatment of human performance may be sufficient to address a PRA application; more realism may not be necessary and could be a waste of resources. However, a conservative approach may not be sufficient when used as the basis for not needing to further investigate the issue at hand. Such an approach could potentially constrain the capability of identifying weaknesses in plant operations and plant practices related to the particular human actions credited in the PRA.

Recognizing that the volume will be used to guide a wide variety of applications, it is not intended that all the practices be met for any specific PRA application; in fact, some may not be applicable or necessary. A practitioner or reviewer should determine the applicable good practices for the PRA application and perform or review the HRA accordingly.

### 1.3 Purpose

This volume serves as a reference guide of good practices in HRA. By good practices we mean those processes and individual analysis tasks and judgments that would be expected of a HRA (considering current knowledge and state-of-the-art) in order for the HRA results to sufficiently represent the anticipated operator performance when making risk-informed decisions. The document is principally focused on the process for performing HRA and does not, for instance, specifically address HRA data or details of specific quantification approaches. As such, it is written in a way that links the prescribed good practices to requirements in the ASME Standard<sup>5</sup> and particularly the HRA section of that document (although nearly all other sections of the standard also have some parallel requirements with regard to operator actions such as in the accident sequence analysis, success criteria, systems analysis, and large early release frequency (LERF) analysis sections).

With this in mind, this volume has at least two primary uses.

1. It provides guidance for performing a good HRA (whether for the first time or when analyzing a change to current plant practices) when implementing the ASME Standard,<sup>5</sup> and focuses on the attributes of a good HRA regardless of the specific methods or tools that are used. The guidance is specifically for HRAs for full power, reactor, and internal events applications although most of the guidance may prove to be useful for other applications (e.g., external events, other operating modes...). It does not endorse nor is it meant to suggest that a specific method or tool be used since many exist, and all have strengths and limitations regarding their use and applicability. Nevertheless, the good practices come from those advocated in such sources as the ASME Standard<sup>5</sup>, THERP<sup>8</sup>, ASEP<sup>12</sup>, SHARP1<sup>13</sup>, SPAR-H Method<sup>14</sup>, and ATHEANA<sup>10</sup> for example, as well as the experiences of the authors and reviewers of this volume.
2. It supports the review of HRAs in assessing the quality of the analyses. In this regard, the practices of a good HRA are provided which should be useful in formulating questions about and measuring the “goodness” of a HRA. Its purpose is not to explicitly provide questions a reviewer should ask, but rather to provide the technical basis for developing questions or a standard review plan for the staff’s review of HRA.

## **2. OVERVIEW OF GOOD PRACTICES FOR HRA**

### **2.1 Scope of HRA Good Practices Guidance**

The purpose of this document on good practices for implementing HRA is to ensure some level of consistency and quality in HRA analyses and their review. In order to achieve such consistency and quality, the HRA good practices in this document are directed at specific HRA tasks or activities.

The performance of HRA typically involves several tasks or activities. Some of these tasks are dependent on the HRA method or quantification approach that is used. Because this HRA good practices document does not endorse or specify the use of specific HRA methods or quantification approaches, most of the guidance in this document is directed at the process for performing HRA. However, this document does provide some non-method-specific good practices with respect to HRA quantification.

As stated in Section 1, the ASME Standard<sup>5</sup> already addresses these HRA tasks or activities at a high level. In the NRC's judgement, the more detailed guidance given in this document on HRA good practices is necessary to achieving acceptable consistency and quality in HRA.

### **2.2 HRA Good Practices and the State-of-the-Art in HRA**

The HRA good practices given in this document are based in part on past experience in performing and reviewing HRAs, including that used to support the IPEs, but also reflect current perspectives on the issues that impact human performance that were gained from developmental projects such as ATHEANA<sup>10</sup>. Consistent with the state of the art in PRAs, it is recommended that future HRA/PRAs attempt to identify and model potentially important EOCs. This report provides some guidance for identifying characteristics of situations that can facilitate errors of commission. As stated above, these good practices apply to the use of all HRA methods and approaches.

### **2.3 Summary and Organization of HRA Good Practices Guidance**

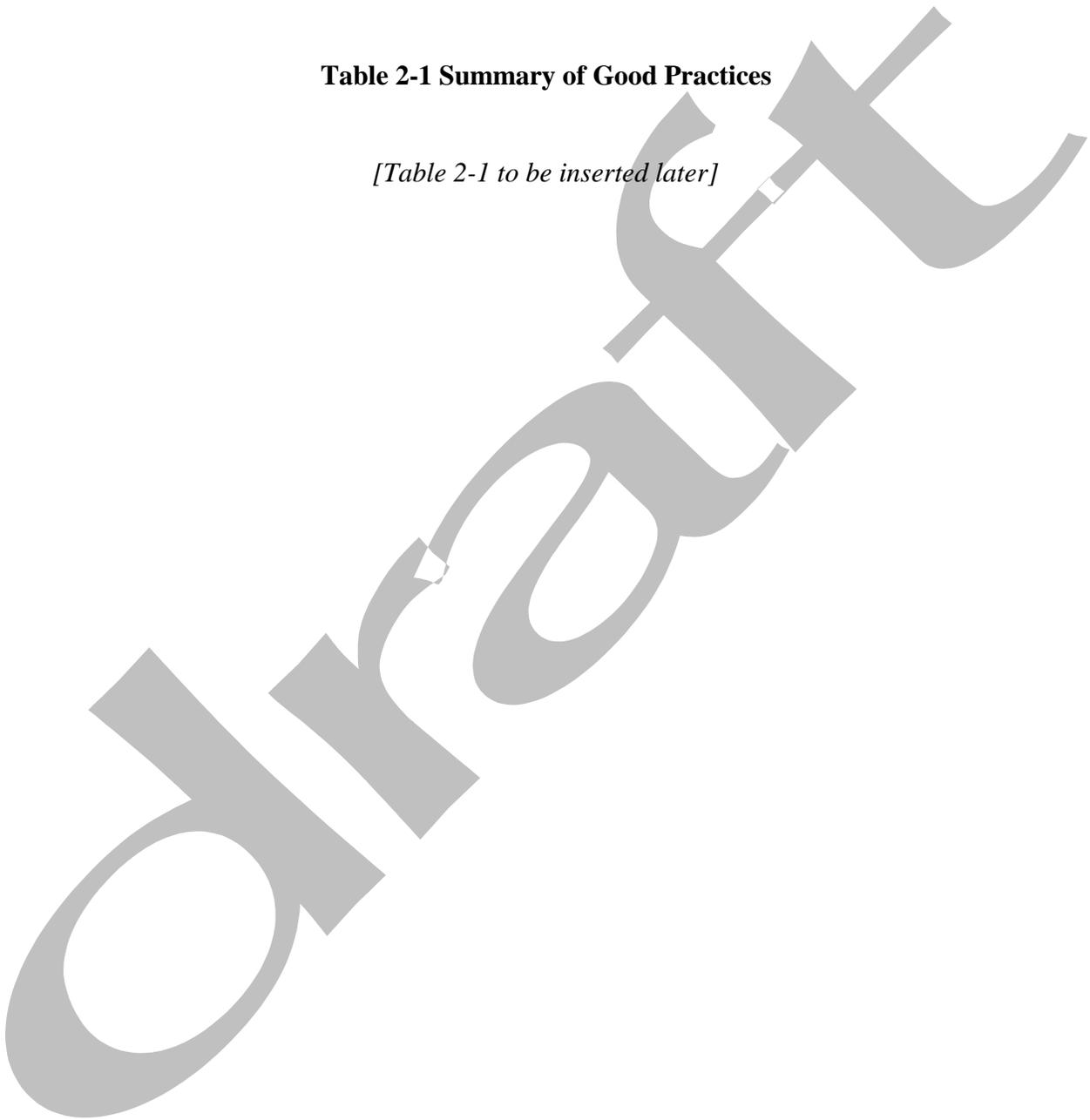
The good practices are presented in a logical analysis approach and linked to the requirements of the ASME Standard.<sup>5</sup> Like the standard, this document specifically addresses pre-initiator (i.e., normal operations) and post-initiator (i.e., emergency operations) human actions since it is assumed that as typical of most PRAs, human actions that cause or contribute to initiating events are already accounted for quantitatively in many initiating event frequencies. Further understanding of specific causes of the initiators is typically not required. It is noted that for support system initiators and other initiators such as those human-induced initiators that may be modeled for other modes (e.g., shutdown), corresponding initiator fault tree models may specifically include human failure events (HFEs) that have characteristics of either pre- or post-initiating event HFEs. The techniques used to analyze these HFEs are therefore covered by this document and should be followed. For example, see HLR-IE-C high level requirement in the ASME Standard<sup>5</sup> and such supporting requirements as IE-C9 concerning the modeling of recovery actions in an initiator fault tree, and IE-C12 concerning procedural influences on the interfacing system loss of coolant accident (ISLOCA) frequency.

While this document is written in a serial fashion, in practice, it is often desirable to perform or review an HRA in a more holistic manner and address multiple steps of the HRA process simultaneously to achieve greater resource efficiency.

Table 2-1 provides brief summaries of the good practices that are discussed in subsequent sections of this document (to be provided later).

**Table 2-1 Summary of Good Practices**

*[Table 2-1 to be inserted later]*



### 3. HRA TEAM FORMATION AND OVERALL GUIDANCE

If human actions are going to be included realistically in the PRA, the modeling of human interactions must consider each action evaluated in the context of a complete accident scenario or sequence of events. To do this, HRA has evolved from the days when PRA analysts provided the human events of interest to a HRA specialist who then assigned human error probabilities (HEPs) to the human events, often in isolation. Such a process is no longer considered good practice. Understanding an accident sequence context is a complex, multi-faceted process. The interaction of plant hardware response and the response of plant operators must be investigated and modeled accordingly. Such characteristics as the following need to be understood and reflected, as necessary, in the model of a specific human action or group of actions:

- plant behavior and conditions,
- 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 sequence ,
- 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, among many other characteristics.

Much of the guidance in this volume is aimed at good practices for understanding the context associated with each modeled human action, and how that context affects both the definition of human failure events and an assessment of their probabilities.

This emphasis on the need to adequately understand and address context in order to more realistically address human performance is based on advances in our understanding of the factors that can influence human performance. These advances come from recent reviews of operational events involving serious accidents (e.g., ATHEANA<sup>10</sup>) and from other international efforts and recent research in the cognitive sciences that together have provided a clearer picture of the ways in which various factors and situations can interact to influence the occurrence of inappropriate human actions (e.g., Reason<sup>15</sup>, Woods<sup>16</sup>, Endsley<sup>17</sup>...). Improvements have been made for how to address the broad range of potential influences on human performance, for both the identification of the human actions to be modeled in the PRA as well as what to consider during screening and detailed quantification of the actions. The guidance in this volume provides good practices that reflect these improvements and ensures the proper treatment of context in performing a reasonably realistic HRA.

Hence, the modeling of human actions in the PRA should involve an integrated effort among PRA modelers, HRA and human factors practitioners, thermal-hydraulic analysts, operations and

maintenance personnel, and sometimes other disciplines depending on the accident sequence (e.g., structural engineers such as if the timing of an action is dependent on when and how the containment might fail). Each discipline provides a portion of the context knowledge. When the context is sufficiently understood, only then can human failure events be realistically modeled and quantified. In addition, as good practice in HRA, it is encouraged that there be the use of walkdowns of areas where the action needs to take place, talk-throughs of the scenarios and actions of interest with plant operators or maintenance personnel, field observations, and at least for the more important actions, simulations of the human actions to be credited. Finally, the HRA should be performed consistently for both core damage prevention/mitigation and large early release prevention/mitigation since both measures are considered in making risk-informed decisions as addressed in Regulatory Guide 1.174<sup>3</sup>.

Therefore, in summary and as the first measure of a good HRA, it should be clear that an HRA assessment has utilized an integrated team and tools as summarized in Table 3-1 to the extent necessary and practical for the PRA application and the specific issue being addressed. This is an important aspect that should lead to HRA results that are credible.

**Table 3-1 Overall HRA Good Practices**

<p>1. The HRA is an integral part of the PRA (not performed as an isolated task in the PRA process) whereby the inputs from the following types of disciplines are used together to define the PRA structure including which human events need to be modeled, how they are defined and modeled in the PRA, and the considerations used to quantify the associated HEPs:</p> <ul style="list-style-type: none"> <li>• PRA modelers</li> <li>• HRA practitioners</li> <li>• Thermal-hydraulic analysts</li> <li>• Operations and maintenance personnel</li> <li>• Other disciplines (e.g., structural engineers, system engineers...) as necessary</li> </ul>
<p>2. Besides the review of plant documents, the HRA is performed using the insights gained from the following to confirm judgments and assumptions made from the document review:</p> <ul style="list-style-type: none"> <li>• Walkdowns of areas where decisions and actions are to take place</li> <li>• Talk-throughs of scenarios and actions of interest</li> <li>• Field observations</li> <li>• Simulator exercises</li> </ul>
<p>3. As part of the integrated effort, the HRA is performed consistently for both core damage and large early release outcomes, since both are equally important in risk-informed applications.</p>

## 4. PRE-INITIATOR HRA

The ASME Standard<sup>5</sup> separates its requirements into two broad classifications; those that address the modeling of failures of pre-initiator human actions and those that address the modeling of failures of post-initiator human actions. This section provides good practices for implementing the requirements for addressing pre-initiator human failure events in a PRA.

Pre-initiator human failure events are events that represent the impact of human failures committed during actions performed prior to the initiation of an accident sequence (e.g., during test or maintenance or the use of calibration procedures). They are important to model because plant personnel can make the equipment needed to mitigate a particular accident sequence unavailable, thus reducing the overall capability to respond to the initiating event. Hence, depending on the issue being addressed, this impact may need to be included in a PRA if a realistic assessment of risk is required.

The following good practices are categorized under four major analysis activities for doing pre-initiator HRA. These analysis activities are:

1. Identifying activities that have the potential to result in pre-initiator human failures
2. Screening out the activities for which human failures do not need to be modeled
3. Modeling specific human failure events (HFEs) corresponding to the unscreened activities
4. Quantifying the corresponding human error probabilities (HEPs) for the specific HFEs.

### 4.1 Identifying potential pre-initiator human failures

4.1.1 **OBJECTIVE:** To identify from routine plant actions, those pre-initiator actions whose failure to perform correctly could result in the human-induced unavailability of PRA-modeled equipment that is credited in the PRA accident sequences. This is important since these actions represent other potential modes of unavailability of the credited equipment (besides the equipment simply failing to start or other failure modes in the PRA) that contribute to overall plant risk. Note that not all the identified actions will be modeled since some may be screened from further analysis in the following analysis activity (screening). The following provides good practices for identifying potential pre-initiator human failures while implementing the related Standard requirements.

#### 4.1.2 CORRESPONDING ASME STANDARD REQUIREMENTS:

The Standard calls for a systematic process to be used to identify routine activities that if not completed correctly, may impact the availability of equipment. There are multiple supporting requirements in the Standard that address the need to consider test and maintenance activities, calibration activities, and actions that could affect multiple equipment.

### 4.1.3 GOOD PRACTICES:

#### 4.1.3.1 Good Practice #1:

The HRA process should include a review of the following:

- All routine (scheduled) test and maintenance as well as calibration procedures that affect equipment to be credited in the PRA (for core damage frequency (CDF) and LERF) should be identified and reviewed.
- Actions specified in the above procedures that realign equipment outside their normal operation or standby status, or otherwise could detrimentally affect the functionality of credited equipment if not performed correctly (e.g., miscalibration) should be identified.
- “Affected” equipment should include (if routinely acted on and credited in the PRA):
  - ▶ the primary systems, structures, and components (SSCs) (e.g., emergency core cooling systems’ components, containment cooling systems’ components...),
  - ▶ support systems (e.g., power, air, cooling water...),
  - ▶ cascading effects among the equipment (e.g., if the realignment of an equipment item in one procedure such as an air-operated valve would implicitly require the subsequent realignment of another equipment item such as isolation of an air line that would then disable a portion of the air system), and
  - ▶ instrumentation (e.g., indicators, alarms, sensors, logic devices...) and controls (e.g., hand switches...) that (a) affect automatic operation of the above primary and support system equipment and/or (b) *at least singularly* are relied upon (as opposed to multiple, redundant items) to credit post-initiator human actions to be included in the model (e.g., a single subcooling indication relied upon to meet an emergency core cooling termination criteria which if miscalibrated could induce failure of the appropriate post-initiator operator action).

#### 4.1.3.2 Good Practice #2:

The identification process should identify pre-initiator human actions even if they may be potentially covered by the affected equipment failure data (see section 4.1.4 for additional information).

#### 4.1.3.3 Good Practice #3:

If applicable and credited in the analysis, the identification process should address other operational modes and routine actions affecting barriers and other structures such as fire doors, block walls, drains, seismic restraints, etc.

#### 4.1.3.4 Good Practice #4:

The identification process needs to include possible pre-initiator actions *at least within each system* where redundant or multiple diverse equipment can be affected by (a) a single act (e.g., misalignment of a valve affecting multiple system trains or even multiple systems) or (b) through a common failure with similar multiple acts (e.g., mis-calibrating multiple sensors due to incorrect implementation of the same calibration procedure or use of the same mis-calibrated standard). For the latter case, the analyst should not duplicate that already covered under the common cause failure modeling of the equipment, but should include consideration of possible commonalities such as:

- same crew, same shift performing the actions (common “who” mechanism),
- common incorrect calibration source (common “what” mechanism),
- common incorrect tool, process, or procedure/training, or inadequate material (e.g., wrong grease) (common “what/how” mechanisms), and
- close proximity in time and/or space/location of similar multiple acts (common “when/where” mechanisms).

The more these commonalities co-exist, the more the identification process should consider the act as a potentially important pre-initiator action to be included.

#### 4.1.4 POSSIBLE IMPACTS OF NOT PERFORMING GOOD PRACTICES AND ADDITIONAL REMARKS:

Besides the obvious issues associated with incompleteness and inaccuracy and thereby potentially missing a risk-significant pre-initiator action, the following observations are noted.

- Missing or unnecessarily including an action is often not a serious mistake (i.e., would not significantly affect the overall risk) unless the action can affect multiple equipment items. This is because with common nuclear plant practices and designs, typically those actions that could affect multiple trains of equipment tend to be the more significant pre-initiator human failures. Those affecting just one equipment item are usually not important unless the equipment item has a high operating reliability (e.g., failure to start or run is in the 1E-4 or lower probability range) and so the pre-initiator failure probability could be a significant contributor to the unavailability of the equipment.
- One should include the possible failures associated with routine test and maintenance or calibration procedures that could affect critical instrumentation, diagnostic devices, or specific items like pushbuttons, etc. that have no redundancy or diverse means of function. While typically such situations do not exist in nuclear power plants, changes to the plant could conceivably and unintentionally create such a situation. Affecting the operator’s ability to take the desired action is similar, functionally, to affecting the equipment item itself which is to be activated. Hence, it at least should be ensured that such situations, from a possible pre-initiator perspective, do not exist or if they do, they are addressed.

- In practice, it is best to include pre-initiator actions even if the associated failure may already be included in the failure data for the affected equipment item (e.g., in the failure-to-start data). This is because it is often hard to determine if the failure data bases include such human failures since data bases are typically insufficiently documented to know if the potential pre-initiator failure is already included. Generally, unless the failure can affect multiple equipment, such failings tend to not be important since missing them or double-counting them tend not to be serious PRA problems. Potential double-counting is the most conservative thing to do, and yet typically not a serious over-estimation of the failure's significance. In addition, including all identified pre-initiators gives analysts the opportunity to identify potentially problematic actions such as those with procedural or training problems, those that do not require appropriate checks, etc.
- If applicable, one should include the possible failures associated with routine test and maintenance or calibration procedures that could affect equipment critical to external events such as fire barriers (e.g., opening a fire door and failing to restore its closed position), seismic restraints, floor drains and barriers, wind barriers, etc. While typically such situations do not exist in nuclear power plants since such equipment items often do not have routine test, maintenance, or calibration activities that would adversely affect their function, changes to the plant or plant practices, for instance, could conceivably and unintentionally create such a situation. To the extent the analysis assumes the functionality of these normally highly reliable devices, pre-initiator failures that could affect these devices could be potentially important. Hence, it at least should be ensured that such situations, from a possible pre-initiator perspective, do not exist or if they do, they are addressed.
- Considering the potential importance of acts that affect multiple equipment, the identification process should search for acts that affect multiple equipment items *at least within a system* (e.g., auxiliary feedwater system, reactor core injection system...) as this represents the current state of the art in PRA. A search across multiple systems (e.g., auxiliary feedwater and high pressure injection) is an expansion of the current state of the art and should not be expected except for those cases where the same instrumentation or equipment (e.g., pressure signals, same tank level equipment) activates or affects multiple systems.

## **4.2 Screening those activities for which human failure events do not need to be modeled**

4.2.1 **OBJECTIVE:** To screen out those activities for which associated failures do not need to be analyzed because they should be probabilistically unimportant. The screening process, though largely qualitative, is based on the belief that certain design or operational practices make some pre-initiator failures sufficiently unlikely that they will not be risk significant failures and therefore do not need to be modeled. The following provides good practices for screening out pre-initiator human actions and associated human failures while implementing the related Standard requirements.

### **4.2.2 CORRESPONDING ASME STANDARD REQUIREMENTS:**

The Standard addresses allowable screening of activities based on practices that limit the likelihood of errors in those activities. There are multiple supporting requirements in the Standard that address screening rules or criteria, as well as the requirement to not screen actions that could affect multiple equipment.

#### 4.2.3 GOOD PRACTICES:

##### 4.2.3.1 Good Practice #1:

A candidate pre-initiator action can be screened out (i.e., not to be modeled) if the nature of the associated action meets any of the following criteria and the reason for screening is documented (see exception under Good Practice #2 below):

- the affected equipment will receive an automatic realignment signal and it can respond (i.e., is not disabled) if demanded, or
- there is a valid post-maintenance/test functional check after the original manipulation which will reveal misalignment or incorrect status (e.g., faulty position, improper calibration), or
- following the original action(s), an independent second verification of equipment status using a written checklist that will verify incorrect status is performed, or
- a valid check, at least once per shift, of equipment status that will reveal misalignment or incorrect status, is used, or
- there is a compelling signal (e.g., annunciator or indication) of improper equipment status or inoperability in the control room, it is checked at least shiftily or daily, and realignment can be easily accomplished, or
- other criteria as long as it can be demonstrated that the resulting human error probabilities would be low compared with the failure probabilities (e.g., failure to open) of the equipment.

##### 4.2.3.2 Good Practice #2:

Do not screen out those actions and possible pre-initiator failures that simultaneously affect multiple (redundant or diverse) equipment items (see Good Practice #4 under Section 4.1.3).

##### 4.2.3.3 Good Practice #3 (application-specific):

For a specific PRA application and depending on the issue being addressed (e.g., examination of a specific procedure change), revisit the original PRA screening process to ensure issue-relevant human actions have not been deleted from the PRA prior to its use to assess the new issue.

#### 4.2.4 POSSIBLE IMPACTS OF NOT PERFORMING GOOD PRACTICES AND ADDITIONAL REMARKS:

Besides the obvious issues associated with inappropriate screening and thereby potentially missing a risk-significant pre-initiator action, the following observations are noted.

- Generally, screening out pre-initiator failures (i.e., don't have to be modeled) is acceptable based on experience with past PRAs and the types of pre-initiator failures that are typically found to be

unimportant. This is done to simplify the model and not expend resources addressing unimportant pre-initiator actions. It should be clear that an appropriate level of investigation has been performed to ensure the above criteria have been met and if these or other criteria are used, their justification is documented for outside review. It is advisable that a record of all screened actions be kept for later reference when performing specific applications (see Good Practice #3). When in doubt, it is recommended the pre-initiator action not be screened out but the corresponding failure modeled in the PRA for further analysis.

- Since pre-initiator actions and related failures affecting multiple equipment items can sometimes be risk important, none of these should be screened out but should be modeled and examined in more detail in the PRA because of the potential consequences of the failure.
- There can be a tendency to want to use an existing PRA model to address issues such as changes to the plant, without spending the appropriate time to revisit some of the underlying assumptions and modeling choices made to create the original PRA. Such a review should be done to see if these assumptions and choices still apply for the issue being addressed. In this case, some pre-initiator failures may not have been included in the original PRA (i.e., screened out) that in light of the new issue being addressed, should now be included in the model (i.e., could be important for addressing the issue). Hence it is good practice to implement a process that ensures that some of the formerly screened out pre-initiator failures do not have to be added back-in to the model in order to appropriately address the issue.

### **4.3 Modeling specific human failure events (HFEs) corresponding to the human failures**

4.3.1 **OBJECTIVE:** To define how the specific pre-initiator HFE is to be modeled in the PRA to accurately represent the failure of each action identified and not screened out from the above analysis activities. The HFE needs to be linked to the affected equipment (single or multiple) and needs to appropriately define the failure mode of that equipment that makes the equipment unavailable. The following provides good practices for modeling pre-initiator human failure events while implementing the related Standard requirements.

#### **4.3.2 CORRESPONDING ASME STANDARD REQUIREMENTS:**

The Standard calls for the modeling of pre-initiator HFEs based on the impact of the failure in the PRA. There are multiple supporting requirements in the Standard that address the modeling level of detail for each HFE and the modes of failure to be considered.

#### **4.3.3 GOOD PRACTICES:**

##### **4.3.3.1 Good Practice #1:**

Define each specific pre-initiator HFE to be modeled in the PRA as a basic event that describes the human-induced failure mode and is located in the model such that it is linked to the unavailability of the affected component, train, system, or overall function (i.e., level of modeling) depending on the effect(s) of the HFE (e.g., a single valve will not close, a train will be isolated, the automatic start

signal for an entire system will be disabled). The following attributes, as a minimum, should be used to define the pre-initiator failure level properly in the PRA:

- the nature of the manipulation affects a whole train, system, etc. so it makes more sense to define the HFE at that level,
- multiple individual acts affecting multiple equipment (e.g., different components) can be combined as a single pre-initiator HFE affecting a higher level of equipment resolution (e.g., the train containing the different components) as long as (a) the acts and effects are related, (b) how the single HFE will be quantified (i.e., the performance-shaping factors that would affect quantification as discussed later) is not significantly different or will be conservatively bounding than if the individual acts were to be modeled and quantified separately, and (c) there are no potential commonalities/dependencies with other pre-initiator acts elsewhere in the model so that potential common failures among similar individual acts might be missed (e.g., miscalibration of multiple signal channels), and
- consideration of the level of detail already modeled in the PRA (e.g., train, system) for failures of the associated equipment (less important factor).

The failure modes (fail to close, fail to start, etc.) should be a direct result of considering the equipment affected and the effects of the human-induced failure (refer to all the Good Practices under Section 4.1.3) and stem from failure to restore equipment and/or otherwise correct the adverse effect (such as miscalibration) so that the equipment is again operable. The failure modes should clearly describe the HFE effect to ensure proper interpretation of the HFE in the model (e.g., only two of three redundant sensors need to be disabled to make the actuation signal unavailable, and not all three sensors have to be disabled).

As an aid to ensure appropriate modeling, it is recommended practice (but not necessary) that the pre-initiator failure be placed in close proximity, in the PRA model, to the equipment affected by the human failure. In this way, a quick comparison can be made between the equipment failure and the pre-initiator human failure to ensure they are consistent.

#### 4.3.4 POSSIBLE IMPACTS OF NOT PERFORMING GOOD PRACTICES AND ADDITIONAL REMARKS:

The precise definition of the pre-initiator basic events and their placement in the model (from both a logic and failure mode standpoints) ultimately define how the model addresses the effects of the human failures. This needs to be done accurately if the model is going to logically represent the real effects of each human failure and if the corresponding HFE is going to be correctly quantified (as discussed later).

### 4.4 Quantifying the corresponding human error probabilities (HEPs) for the specific HFEs

4.4.1 OBJECTIVE: To address how the human error probabilities (HEPs) for the modeled HFEs from the previous analysis activity are to be quantified. This section provides good practices guidance on an attribute or criteria level and does not endorse a specific tool or technique

(although THERP<sup>3</sup> or its ASEP<sup>4</sup> simplification are among those often used). Ultimately, it is these probabilities along with the other equipment failure and post-initiator human error probabilities as well as initiating event frequencies that are all combined to determine such risk metrics as CDF, LERF,  $\Delta$ CDF,  $\Delta$ LERF, etc. as addressed in Regulatory Guide 1.174<sup>11</sup>. The following provides good practices for quantifying pre-initiator human failure events while implementing the related Standard requirements.

#### 4.4.2 CORRESPONDING ASME STANDARD REQUIREMENTS:

The Standard calls for a systematic process for assessing the pre-initiator HEPs that addresses plant-specific and activity-specific influences. There are multiple supporting requirements in the Standard that address many factors associated with quantifying the HEPs. These include when screening vs. detailed estimates are appropriate, performance-shaping factors considered in the evaluations, treatment of recovery, consideration of dependencies among HFEs, uncertainty, and reasonableness of the HRA results.

#### 4.4.3 GOOD PRACTICES:

##### 4.4.3.1 Good Practice #1:

The use of screening-level human error probability (HEP) estimates is virtually necessary during the early stages of PRA development and quantification. This is acceptable (and almost necessary since not all the potential dependencies among human events can be pre-known) provided (a) it is clear that the individual values used are over-estimations of the probabilities if detailed assessments were to be performed AND (b) dependencies among multiple human failure events appearing in an accident sequence are conservatively accounted for. These screening values should be set so as to be able to make the PRA quantification process more efficient (by not having to perform detailed analysis on every human failure event), but not so low that later detailed analysis would actually result in higher HEPs. The screening estimates should consider both individual HEPs and the potential for multiple and possibly dependent human failure events for a given accident sequence (scenario). To meet these conditions, it is recommended that (unless a more detailed assessment is performed of the individual or combination events to justify lower values):

- no individual pre-initiator HEP screening value should be lower than 1E-2 (typical of highest pre-initiator values in PRAs), and
- multiple HEPs in the same sequence should not have a collective value lower than 5E-3 (accounts for a 0.5 high dependency factor) at this stage.

##### 4.4.3.2 Good Practice #2:

As needed for the issue being addressed to produce a more realistic assessment of risk, detailed assessments (not just screening estimates) of at least the significant human failure event contributors should be performed. The PRA analyst can define the significant contributors by use of typical PRA criteria (not addressed here) such as importance measure thresholds as well as other qualitative and

quantitative considerations. While the use of screening-level values (supposedly purposely conservative) may, at first, seem to be a “safe” analysis process, it can have negative impacts. Screening values can focus the risk on inappropriate human actions or related accident sequences and equipment failures because of the intentionally high HEPs. Such incorrect conclusions need to be avoided by ensuring a sufficient set of more realistic, detailed HEPs are included in the model.

#### 4.4.3.3 Good Practice #3 (application-specific):

For a specific PRA application and depending on the issue being addressed (e.g., examination of a specific procedure change), revisit the use of screening vs. detail-assessed HEPs to ensure issue-relevant human actions have not been prematurely deleted from the PRA or there is an inappropriate use of screening vs. detailed values to properly assess the issue and the corresponding risk.

#### 4.4.3.4 Good Practice #4:

HEP assessments should account for the most relevant plant-specific and activity-specific performance-shaping factors in the analysis of each pre-initiator HFE. There is not one consensus list of appropriate contextual factors (e.g., plant conditions, PSFs, activity characteristics, etc.) to be considered in the evaluation of the pre-initiator HEPs. Additionally, for a specific action, what factors are most relevant may be different (e.g., perhaps one act is time-sensitive because it is done in a high radiation area while another is most affected by the complexity of steps with many opportunities to make undetected mistakes). It should be qualitatively apparent that the factors seemingly most relevant to the act (based on an understanding of the act) have been considered in the corresponding HEP estimate.

Factors that are typically important to address because they tend to be variable and not almost always optimal based on typical nuclear plant practices, include:

- whether written work plans, job briefs, and related procedures (positive influences tending to lower the HEP), or verbal guidance and/or memory (more negative influences tending to raise the HEP) are used, as well as the quality of the information (e.g., look for ambiguities, incompleteness, inconsistencies, etc. that are negative influences and thus tend to raise the HEP),
- complexity (e.g., multiple and/or repetitive steps that are hard to track, use (or not) of checklists, several variables involved and calculations required...), and
- ergonomic issues (e.g., layout, available information [instruments, alarms, computer readouts, etc.], labeling, readability, highly physical...).

Other factors that tend to not be as important either because of typical nuclear plant practices or because the factors are typically less relevant include (it should still be ensured that the typical practice or irrelevancy is not compromised):

- skill level/experience/training of crew (typically adequate in nuclear plants for the jobs each crew member is to perform),

- stress level (not usually relevant in pre-initiator failures unless special situations such as potential personal harm, the need for fast sequential responses, etc. play a role),
- environmental factors such as temperature, humidity, radiation, noise, lighting, etc. (typically the environment is sufficiently benign except for special circumstances such as a high radiation environment and thus the desire to hurry the actions), and
- availability of time (not usually a strong factor in pre-initiator failures).

If the large majority of these factors affect the human performance negatively or if even just one or two is an overwhelming negative influence, the HEP will tend to be higher (e.g., 0.01 to 0.1 or even higher, not accounting for recovery addressed under Good Practice #5 below). Conversely, mostly positive influences should yield lower HEPs (e.g.,  $<1E-3$ , with additional recovery factors still to be applied as addressed under Good Practice #5 below).

#### 4.4.3.5 Good Practice #5:

Applicable recoveries applied to the HEP evaluations for the HFES being analyzed should be used (multiple recoveries may be acceptable) where appropriate, but any dependencies among the initial failure and the recoveries, and among the recoveries themselves, must be considered (see Good Practice #6 below). Typical considerations in applying recovery include:

- post-maintenance or post-calibration tests are required and performed by procedure,
- independent verification, using a written check-off list, which verifies component status following maintenance/testing/calibration is used, and its practice has been verified by walk-throughs and examination of plant experience,
- the original performer, using a written check-off list, makes a separate check of component status at a later time,
- work shift or daily checks are performed of component status, using a written check-off list,
- there is a compelling feedback (e.g., alarm) that will enhance the original failure being detected and can be quickly recovered, or
- combinations of the above.

The more of these are applicable for a given pre-initiator HFES, the more the situation tends to increase the recovery potential (i.e., decrease the HEP) since each recovery, to the extent they are independent, result in a multiplier (e.g., 0.1) on the original HEP estimate thereby reducing its overall value.

Basic HEPs for pre-initiator HFES for nuclear plant applications (including recovery) are typically expected in the 0.01 (among the highest) to 0.0001 range. Any values below the 0.0001 to 0.00001 range should be considered suspect unless justified.

#### 4.4.3.6 Good Practice #6:

Dependencies among the pre-initiator HFEs and hence the corresponding HEPs in an accident sequence should be quantitatively accounted for in the PRA model. This is particularly important so that combined probabilities are not inadvertently too optimistic, resulting in the inappropriate decrease in the risk significance of human actions and related accident sequences and equipment failures. In the extreme, this could result in the inappropriate screening out of accident sequences from the model because the combined probability of occurrence of the events making up an accident sequence drops below a threshold value used in the PRA to drop sequences from the final risk results.

To address these dependencies, usually a level or degree of dependence among the HFEs in an accident sequence is determined, at first qualitatively (e.g., low, high, complete), and then combined HEPs are assessed accordingly. Once the first HEP has been estimated, subsequent quantitative factors for dependent human failures or recoveries of the original failure are typically expected to be:

- 0.01 to 0.1 for low dependence
- 0.1 to 0.5 for high dependence
- >0.5 for very high or 1.0 for complete dependence

Note that specific tools/techniques may use somewhat different probabilities than provided here based on specific considerations.

In establishing the level of dependence, Good Practice #4 under Section 4.1.3 addresses typical commonalities that tend to make HEPs more dependent (i.e., an HFE is not independent of another HFE and so once the first human failure occurs, there is a high likelihood that a similar second or third, etc. human failure will also occur such as the failure to restore the lineup of one train of equipment after a test and then failing to similarly restore the second train of equipment after a similar test). Good Practice #5 just above addresses recovery characteristics that tend to break-up these commonalities because they “recover” any initial error, making the individual HFEs more independent. The more the types of commonalities addressed under Good Practice #4 under Section 4.1.3 exist and the less corresponding recoveries under Good Practice #5 above exist, the higher should be the assessed level of dependence among the HFEs. To the extent the converse is true, low or even no dependence should be assessed.

#### 4.4.3.7 Good Practice #7:

Point estimates should be mean values for each HEP (excluding screening HEPs) and an assessment of the uncertainty in the mean values should be performed at least for the dominant HEPs to the extent that these uncertainties need to be understood and addressed in order to make appropriate risk-related decisions. Assessments of uncertainty are typically performed by:

- assigning uncertainty distributions for the HEPs and propagating them thru the quantitative analysis of the entire PRA such as by a Monte Carlo technique, and/or
- performing sensitivity analyses that demonstrate the effects on the risk results for extreme estimates in the HEPs based on at least the expected uncertainty range about the mean value.

Note, in some cases, it may be sufficient to address the uncertainties by just qualitative arguments without the need to specifically quantify them (e.g., justifying why the HEP cannot be very uncertain or why a change in the HEP has little relevancy to the risk-related decision to be made).

In assessing the uncertainties, and particularly when assigning specific uncertainty distributions, the uncertainties should include (a) those epistemic uncertainties because of lack of knowledge of the true expected performance of the human for a given context and associated set of performance-shaping factors, and (b) consideration of the combined effect of the relevant aleatory (i.e., random) factors to the extent they are not specifically modeled in the PRA and to the extent that they could alter the context and performance-shaping factors for the HFE. For pre-initiator HFEs, there should be few or no aleatory factors worthy of consideration, since typically the procedure used, the environment experienced, etc. do not randomly change. But, for example, if different and significant crew experience levels are known to exist, it is random as to which crew will perform the pre-initiator act at any given time. In such a case, the mean should represent the average crew experience level and the uncertainty should reflect the possible range in those levels. Again, aleatory factors are typically not very relevant to pre-initiator HEPs and so typically are not important to address.

Whatever uncertainty distributions are used, the shape of the distributions (e.g., log-normal, normal, beta...) are typically unimportant to the overall risk results (i.e., the results are usually not sensitive to specific distributions). Further, typical uncertainties include values for the HEP that represent a factor of 10 to 100 between the lower bound value and the upper bound value that encompass the mean value.

#### 4.4.3.8 Good Practice #8:

The pre-initiator HEPs (excluding the screening HEPs) should be reasonable from two standpoints:

- first and foremost, relative to each other (i.e., the probabilistic ranking of the failures when compared one to another), and
- in absolute terms (i.e., each HEP value) to the extent that the sensitivity of the risk-related decision is not important as to the absolute values for the HEPs.

This reasonableness should be checked based on consideration of actual plant experience and history, against other evaluations (such as for similar acts at other plants), and the qualitative understanding of the actions and the relevant contexts and performance-shaping factors under which the acts are performed. It is suggested that a rank-ordered list of the pre-initiator HFEs by probability be used as an aid for checking reasonableness. For example, simple, procedure-guided, independently checked actions should have lower HEPs than complex, memorized, not checked actions, all other factors being the same. Typical expectations of pre-initiator HEPs can be wide-spread (~0.01 to 0.0001) and depend particularly on the relevant contextual factors, applicable recoveries, and proper consideration of dependencies as discussed under many of the Good Practices covered above.

#### 4.4.4 POSSIBLE IMPACTS OF NOT PERFORMING GOOD PRACTICES AND ADDITIONAL REMARKS:

Besides the obvious concerns about inaccuracies in the HEP quantification and thus whether the HEPs “make sense”, as well as the resulting potential misinformation about the dominant risk contributors if quantification is not done well, the following observations are noted.

- Screening is a useful and most often, necessary part of HRA so as to avoid the expenditure of resources on unimportant human events and accident sequences. The above guidance is aimed at allowing a level of useful screening without inadvertently and inappropriately allowing the analytical phenomenon of, for instance, multiplying three human events in the same sequence each at a screening value of 1E-2 to yield a 1E-6 combined probability, without checking for dependencies among the human events. In such a case some human failure events and combinations of events, or even whole accident sequences, may inappropriately screen out of the PRA model entirely because the accident sequence frequency drops below a model threshold. Hence some of the dominant individual or combination contributors may be missed. This is why the screening values both individually and for combined events should not be too low during the screening stage. Further, if screening values are left permanently assigned to some human failure events that should be assessed with more detail to obtain a more realistic assessment of risk (supposedly lowering the probability), the risk significance of these human failure events and related equipment failures are likely to be over-emphasized at the expense of improperly lessening the relative importance of other events and failures.
- It is important to be sure that dependencies among the various modeled HFEs including the associated recoveries, have been investigated (e.g., the same person as the originator of the action performing the recovery may be more prone to fail to detect the original failure than an independent checker). Treating HFEs and any corresponding recoveries as independent acts without checking for dependencies (thereby being able to multiply the individual HEPs) can inappropriately lessen the risk significance of those HFEs and related equipment failures in accident sequences. This can cause the inappropriate dropping out of accident sequences because the sequences quantitatively drop below a model threshold value as discussed above under screening. Proper consideration of the dependencies among the human actions in the model is necessary to reach the best possible evaluation of both the relative and absolute importance of the human events and related accident sequence equipment failures.
- The use of mean values and addressing uncertainties are a part of the Regulatory Guide 1.174<sup>11</sup> guidance and to the extent addressed therein, the HRA quantification needs to be consistent with that guidance when making risk-informed decisions.
- There can be a tendency for analysts to want to use an existing PRA model to address issues such as changes to the plant, without spending the appropriate time to revisit some of the underlying assumptions and modeling choices made to create the original PRA. A review should be done to see if these assumptions and choices still apply for the issue being addressed. In this case, some pre-initiator human failure events may be quantified in the original model using a set of screening estimates and detailed failure probabilities that may not be appropriate for the new issue being addressed. As an example, where higher screening values may have been acceptable for purposes of the original PRA, these supposedly conservative values may over-estimate the contribution of

these human failure events for the issue being addressed. Further, the relative risk contribution of equipment and associated accident sequences with which the human failure events appear, may be artificially too high (and therefore other events too low) because of the screening values. Hence it is good practice to revisit the use of screening and detailed human failure event probabilities in order to appropriately address the issue.

draft

## 5. POST-INITIATOR HRA

The ASME Standard<sup>5</sup> separates its requirements into two broad classifications; those that address the modeling of failures of pre-initiator human actions and those that address the modeling of failures of post-initiator human actions. This section provides good practices for implementing the requirements for addressing post-initiator human failure events (HFEs) in a PRA.

Post-initiator human failure events are events that represent the impact of human failures committed during actions performed in response to the initiation of an accident sequence (e.g., while following post-trip procedures or performing other recovery actions). They are important to model because humans can have a direct influence on the mitigation or exacerbation of undesired plant conditions after the initial plant upset. Hence, depending on the issue being addressed, this impact may need to be included in a PRA if a realistic assessment of risk is required.

The following good practices are categorized under four major analysis activities for doing post-initiator HRA. These analysis activities include:

1. Identifying potential post-initiator human failures
2. Modeling specific human failure events (HFEs) corresponding to the human failures
3. Quantifying the corresponding human error probabilities (HEPs) for the specific HFEs
4. Adding recovery actions to the PRA.

### 5.1 Identifying potential post-initiator human failures

5.1.1 **OBJECTIVE:** To identify the key human response actions that may need to be taken by the operators in response to a variety of possible accident sequences and that will therefore need to be modeled in the PRA. This is important since failures associated with these actions (e.g., failure to start standby liquid control, failure to initiate feed and bleed, failure to properly control steam generator feed flow, failure to align containment/suppression pool cooling) are represented in the PRA such that in combination with equipment failures, are expected to lead to core damage and/or large early releases. Such failures contribute to the overall risk and thus a systematic process needs to be followed to identify these response actions. The following provides good practices for identifying post-initiator human failures while implementing the related Standard requirements.

#### 5.1.2 CORRESPONDING ASME STANDARD REQUIREMENTS:

The Standard calls for a systematic review to identify operator responses required for each of the accident sequences. There are multiple supporting requirements in the Standard that address what to review as well as the types of actions to be included. Use of talk throughs and simulator observations are also addressed as part of the supporting requirements.

### 5.1.3 GOOD PRACTICES:

#### 5.1.3.1 Good Practice #1:

Reviews of the following form the primary bases for identifying the post-initiator actions.

- Review plant-specific emergency operating procedures (EOPs), abnormal operating procedures (AOPs), annunciator procedures, system operating procedures, severe accident management guidelines (SAMGs), and other special procedures (e.g., fire emergency procedures) as appropriate. The review is done to identify ways operators are intended to interact with the plant equipment after an initiator as a function of the various conditions that can occur as defined by the development of the PRA accident sequences and equipment unavailabilities and failure modes. Particularly note where operator actions are called out in these procedures and under what plant conditions and indications (cues) such actions are carried out. It will also be useful at this time to examine whether there are any potential accident conditions under which the procedures might not match the situation as well as would be desired, e.g., potentially ambiguous decision points or incorrect guidance provided under some conditions. Information about such potential vulnerabilities will be useful later during quantification and may help identify actions that need to be modeled.

While not necessary at this stage of the analysis (probably more beneficial during the modeling and quantification phases, but could be started at this stage on a selective basis of likely importance), the results of the following additional reviews may add to the list of actions and/or help interpret how procedural actions should be defined based on how they are actually carried out.

- Review of training material including, where possible, talk-throughs or walkdowns of the actions with operations or training staff to ensure consistency with training policies and teachings, and to identify likely operator response tendencies for various conditions that may not be evident in the procedures (although it is not the intent to perform numerous or detailed talk-throughs, walkdowns, or simulations at this phase of the analysis - the use of these techniques is more relevant later under the HFE modeling and quantification phases). For example, operators may cite a reluctance to restart reactor coolant pumps in spite of the procedure direction based on their training and perceived adverse effects, or they may have a preference to use condensate as a BWR injection source before using lower pressure emergency core cooling system. These added “interpretations” of the procedures can help complete and/or clarify the identified actions and ensure that later modeling and quantification of the actions will reflect the “as-operated” plant.
- Observations of simulated accidents since these can provide valuable insights with regard to how the actions are actually carried out, by whom, and particularly how procedure steps are interpreted by plant crews especially where the procedure is ambiguous or leaves room for flexibility in the crew response (although it is not the intent to perform numerous or detailed talk-throughs, walkdowns, or simulations at this phase of the analysis - the use of these techniques is more relevant later under the HFE modeling and quantification phases). For example, through simulation it may be observed that a “single action” in the procedure (e.g., align recirculation) is actually carried out by a series of numerous and sequential individual actions (e.g., involving the use of many handswitches in a certain sequence). Again these observed “interpretations” of the procedures can help complete and/or clarify the identified actions and ensure that later modeling

and quantification of the actions will reflect the “as-operated” plant.

#### 5.1.3.2 Good Practice #2:

The review process should involve the following:

- Knowledge of the functions and associated systems and equipment to be modeled in the PRA for both CDF and LERF.
- Identifying whether the function is needed (e.g., injection) or undesired (e.g., stuck-open safety relief valve) recognizing these may vary with different initiators and sequences.
- Identifying the systems/equipment that can contribute to performing the function or cause the undesired condition including structures and barriers where appropriate (e.g., fire door, floor drains) especially for external event analyses.
- Identifying ways the equipment can functionally succeed (i.e., the success criteria) and fail.
- Based on the above, identifying ways the operators are (a) intended/required to interact with the equipment credited to perform the functions modeled for the accident sequences modeled in the PRA and/or (b) to respond to equipment and failure modes that can cause undesired conditions per the PRA. During the identification process, it is helpful to use action words such as actuate, initiate, isolate, terminate, control, change, etc. so that the desired actions are clear.

#### 5.1.3.3 Good Practice #3:

While the specific actions to be identified may be plant-specific, in general, the following types of actions are expected to be identified. Note that actions that are heroic (e.g., must enter an extreme high radiation environment) or without any procedure guidance or not trained on, should not be included or credited in the analysis (exceptions may be able to be justified, but this should not be normal practice).

- Include necessary and desired/expected actions (e.g., initiate RHR, control vessel level, isolate a faulted steam generator, attempt to reclose a stuck-open relief valve).
- Include backup actions to failed automatic responses (e.g., manually start a diesel generator that should have auto started) but be sure the action can be credited to recover the auto failure mode.
- Include anticipated procedure-guided or skill-of-the-craft recovery actions (e.g., restore offsite power, align firewater backup) although these may best be defined later as the PRA quantification begins and important possible recovery actions become more apparent.

Consistent with present day state-of-the art, acts whose failure involve an error of omission (EOO) should be included when identifying post-initiator acts of concern. These involve failure to take the appropriate actions as called out in the procedures and/or trained on or expected as common practice. For example, failure to initiate feed and bleed or failure to start standby liquid control, are EOOs. Possible acts whose failure would involve an error of commission (EOC) are generally beyond current

PRA practice. These involve performing expected acts incorrectly or performing extraneous and detrimental acts such as shutting down safety injection when it is not appropriate. These are not necessarily expected to be identified but see Section 7 of this document for more on this subject.

Finally, it should be recognized that iterations as well as refinement and review of the PRA model construction may (and often do) provide additional opportunities to identify any potentially important missed actions as the PRA model evolves.

#### 5.1.4 POSSIBLE IMPACTS OF NOT PERFORMING GOOD PRACTICES AND ADDITIONAL REMARKS:

While not all the post-initiator actions will be important in the final assessment of risk, unlike the pre-initiator actions, it is difficult to predetermine (at this stage) a set of actions that do not have to be included as part of the identification process. Ways the operators interact with the plant and affect the outcome of any accident sequence need to be assessed in order to determine their relative significance. Hence the good practices herein are aimed at ensuring potentially risk-significant post-initiator actions (based on the procedures as well as the ways the procedures are interpreted and carried out) are identified at this stage of the analysis. Otherwise, the model could be incomplete and/or inaccurate, potentially resulting in misinformation as to the risk dominant plant features (including the important human actions).

### 5.2 Modeling specific human failure events (HFEs) corresponding to the human failures

5.2.1 **OBJECTIVE:** To define how each specific post-initiator HFE is to be modeled in the PRA to accurately represent the failure of each action identified. This involves the modeling of the HFEs as human-induced unavailabilities of functions, systems, or components consistent with the level of detail in the PRA accident sequences and system models, possible grouping of responses into one HFE, and ensuring the modeling reflects certain plant-specific and accident sequence-specific considerations. The following provides good practices for modeling post-initiator human failure events while implementing the related Standard requirements.

#### 5.2.2 CORRESPONDING ASME STANDARD REQUIREMENTS:

The Standard calls for the HFEs to be defined so that they represent the impact of not properly performing the required responses, consistent with the structure and level of detail of the accident sequences. There are multiple supporting requirements in the Standard that address the modeling level of detail for each HFE and how to complete the definition of each HFE.

#### 5.2.3 GOOD PRACTICES:

##### 5.2.3.1 Good Practice #1:

Define each specific post-initiator HFE to be modeled in the PRA as a basic event that describes the human failure of not properly performing the required response and is located in the model such that it is linked to the unavailability of the affected component, train, system, or overall function (i.e., level of modeling) depending on the effect(s) of the HFE (e.g., failure to manually depressurize using the

safety relief valves, failure to manually scram, failure to align the backup train of service water). The following considerations should be used to define the post-initiator failure level properly in the PRA:

- the nature of the action is performed on a train, system, etc. level so it makes more sense to define the HFE at that level,
- the consequences of the failure and what would be affected by the failure (just a component is affected, a whole train, a system, multiple systems, an entire function),
- multiple individual acts/responses such as at a system or component level (e.g., starting high pressure injection and then subsequently opening a power-operated pressurizer relief valve) can be combined as a single post-initiator HFE affecting a higher level of equipment resolution such as at a system or a function level (e.g., initiating feed and bleed) as long as (a) the acts and effects are related, (b) how the single HFE will be quantified (i.e., the performance-shaping factors that would affect quantification as discussed later) is not significantly different or will be conservatively bounding than if the individual acts were to be modeled and quantified separately, and (c) there are no potential commonalities/dependencies with other post-initiator acts elsewhere in the model so that potential common failures among similar individual acts might be missed (see the discussion presented below),
- the level of detail already modeled in the PRA (train, system, etc.) for failures of the associated equipment (less important factor).

As an example of how human responses may be grouped and modeled as one or more HFEs, consider the case in a boiling water reactor (BWR) of a desired response to control reactivity in an anticipated transient without scram scenario. Failure to control reactivity could be defined as one HFE, or as several HFEs based on the subtasks involving inhibiting the automatic depressurization system, lowering reactor water level, and initiating the standby liquid control system.

For situations such as the above example, if failure to perform the subtasks (a) have different effects, (b) may individually be impacted by very different performance-shaping factors (e.g., in-control room actions vs. local actions in a high steam environment area, a subtask performed early in the scenario vs. another subtask performed much later in the scenario), or (c) involves an action that has a dependency with some other action to be modeled in the PRA (e.g., failure to trip two reactor coolant pumps followed by subsequent failure to trip the remaining reactor coolant pumps when conditions warrant), the failures are best modeled as separate HFEs. An alternative is to model them all as one HFE and model the bounding consequence (such as the failure to control reactivity example cited above) as long as the most limiting performance-shaping factors are used (e.g., the shortest time that any of the subtasks must be performed, the most complex of the subtasks, etc.) and any subtask dependencies with other HFEs are identified, treated in the model, and properly quantified.

The failure effects as depicted in the PRA model should be a direct result of considering the equipment affected and the effects of the human-induced failure (refer to the Good Practices under Section 5.1.3) and stem from failure to properly perform the correct responses. The failures should sufficiently describe the HFE and its effect to ensure proper interpretation of the HFE in the model (e.g., fail to initiate feed and bleed within 5 minutes of the reactor pressure achieving 2400 psig).

As an aid to ensure appropriate modeling, it is recommended practice (but not necessary) that the post-initiator failure be placed in close proximity, in the PRA model, to the component, train, system, or

function affected by the human failure. In this way, a quick examination of the model can reveal the modeled effect of the human failure.

#### 5.2.3.2 Good Practice #2:

Each of the modeled post-initiator HFEs should be defined such that they are plant- and accident sequence-specific. Where helpful to fully understand the nature of the act(s) (e.g., who performs it, what is done, how long does it take, are there special tools needed, are there environmental issues or special physical needs, etc.), use of talk-throughs, walkdowns, field observations, and simulations are particularly encouraged.

In order for the act to occur, the operator must diagnose the need to take the act and then execute the act. While many performance-shaping factors are used to quantify the probability for failing to perform the act correctly (as discussed later under quantification), all of which should be evaluated based on plant and accident sequence-specifics, the following requirements are particularly germane to a basic understanding of the HFE and should be met to complete the definition of each HFE:

- to the extent possible, the time by which the act needs to be performed (e.g., fail to initiate feed and bleed by 2 minutes after primary pressure reaches 2400 psig), and the time necessary to diagnose the need for and to perform the act (1 minute) should be based on plant and accident sequence-specific timing and nature of the complexity and/or subtasks involved in implementing the act (i.e., not another plant analysis or a general analysis for the “average” plant since the number and nature of the specific manipulations could be different, the plant thermal hydraulic response could be different, the location for local actions may require different travel times, some sequences require a fast response while others may require a much quicker response for the same act, etc.),
- similar to the above, the availability and timing of plant and accident sequence-specific cues (i.e., indications, alarms, visual observations, etc. and when they will be manifested) should be used as these can be different from plant-to-plant and different in a variety of accident sequences (e.g., such as a DC bus failure causing loss of some indications or alarms), and will affect the likelihood and timing of diagnosing the need for the action,
- plant-specific procedure and training guidance should be used based on the reviews under the Good Practices in Section 5.1.3,
- where the act is performed (e.g., in the control room, locally in the auxiliary building) should be noted, and
- the use of walkdowns, talk-throughs, and field or simulator observations are encouraged when defining the HFE as mentioned under Good Practice #1 under Section 5.1.3. See more about the benefits of these techniques in Appendix A.

#### 5.2.4 POSSIBLE IMPACTS OF NOT PERFORMING GOOD PRACTICES AND ADDITIONAL REMARKS:

The precise definition of the post-initiator basic events and their placement in the model (from both a logic and failure mode standpoints) ultimately define how the model addresses the effects of the

human failures. This needs to be done accurately if the model is going to logically represent the real effects of each human failure and if the corresponding HFE is going to be correctly quantified (as discussed later). This accuracy is best obtained if plant-specific and accident sequence-specific information is used. Nevertheless, the following observation is noted.

- Not using plant/accident sequence-specific thermal hydraulic information for timing may or may not be critical based on the relevancy and thus appropriateness of the non-specific (i.e., “general”) timing information that is used. It is better to use plant and accident-specific information, though it is recognized that in some areas (e.g., containment response for LERF), from a practical standpoint, modified “general” information may be all that is readily available. Further, as long as the timing considerations used are reasonable and accurate to within the resolution of the HRA quantification tool to be used, differences between plant and accident-specific vs. more “general” timing considerations may not be a significant issue. Analysts should ensure that if non-specific timing information is used, it is reasonable to expect it to be appropriate for the plant and accident sequence being analyzed.

### **5.3 Quantifying the corresponding human error probabilities (HEPs) for the specific HFEs**

5.3.1 **OBJECTIVE:** To address how the human error probabilities (HEPs) for the modeled HFEs from the previous analysis activity are to be quantified. This section provides good practices guidance on an attribute or criteria level and does not endorse a specific tool or technique. Ultimately, it is these probabilities along with the other equipment failure and pre-initiator human error probabilities as well as initiating event frequencies that are all combined to determine such risk metrics as CDF, LERF,  $\Delta$ CDF,  $\Delta$ LERF, etc. as addressed in Regulatory Guide 1.174<sup>11</sup>. The following provides good practices for quantifying post-initiator HEPs while implementing the related Standard requirements.

#### **5.3.2 CORRESPONDING ASME STANDARD REQUIREMENTS:**

The Standard requires that a well-defined and self-consistent process be used to quantify the post-initiator HEPs. There are multiple supporting requirements in the Standard that address many factors associated with quantifying the HEPs. These include when conservative vs. detailed estimates are appropriate, consideration of cognitive and execution failures, performance-shaping factors considered in the evaluations, consideration of dependencies among HFEs, uncertainty, and reasonableness of the HRA results.

#### **5.3.3 GOOD PRACTICES:**

##### **5.3.3.1 Good Practice #1:**

Whether using conservative or detailed estimation of the post-initiator HEPs, the evaluation should include both cognitive (i.e., “thinking”) as well as execution failures. For example, incorrectly interpreting a cue or not seeing a cue and thus not performing the act can be one mode of failure. Or, the operator can intend to take the act based on the proper and recognized cues but still otherwise fail to take the act or perform it correctly. Both need to be part of the HEP evaluations.

#### 5.3.3.2 Good Practice #2:

The use of conservative human error probability (HEP) estimates is virtually necessary during the early stages of PRA development and quantification. This is acceptable (and almost necessary since not all the potential dependencies among human events can be pre-known) provided (a) it is clear that the individual values used are over-estimations of the probabilities if detailed assessments were to be performed AND (b) dependencies among multiple human failure events appearing in an accident sequence are conservatively accounted for. These conservative values should be set so as to be able to make the PRA quantification process more efficient (by not having to perform detailed analysis on every human failure event), but not so low that later detailed analysis would actually result in higher HEPs. The conservative estimates should consider both individual HEPs and the potential for multiple and possibly dependent human failure events for a given accident sequence (scenario). To meet these conditions, it is recommended that (unless a more detailed assessment is performed of the individual or combination events to justify lower values):

- no individual post-initiator HEP conservative value should be lower than the worse case anticipated detailed value and generally not lower than 0.1 (typical of high post-initiator values in PRAs), and
- multiple HEPs in the same sequence should not have a joint probability value lower than the worse case anticipated detailed joint probability value and generally not lower than  $5E-2$  (accounts for a 0.5 high dependency factor) at this stage.

#### 5.3.3.3 Good Practice #3:

As needed for the issue being addressed to produce a more realistic assessment of risk, detailed assessments (not just conservative estimates) of at least the dominant human failure event contributors should be performed. The PRA analyst can define the dominant contributors by use of typical PRA criteria (not addressed here) such as importance measure thresholds as well as other qualitative and quantitative considerations. While the use of conservative values may, at first, seem to be a “safe” analysis process, it can have negative impacts. Conservative values can focus the risk on inappropriate human actions or related accident sequences and equipment failures because of the intentionally high HEPs. Such incorrect conclusions need to be avoided by ensuring a sufficient set of more realistic, detailed HEPs are included in the model.

#### 5.3.3.4 Good Practice #4 (application-specific):

For a specific PRA application and depending on the issue being addressed (e.g., examination of a specific procedure change), revisit the use of conservative vs. detail-assessed HEPs to ensure issue-relevant human actions have not been prematurely deleted from the PRA or there is an inappropriate use of conservative vs. detailed values to properly assess the issue and the corresponding risk.

#### 5.3.3.5 Good Practice #5:

As “good practice,” the following table of performance-shaping factors (Table 5-1) for both in-control room and ex-control room (local) actions should be treated in the evaluation of each HEP per the table guidance. The guidance should fit most cases, but it should be recognized that for specific actions,

some of the factors may not apply while others may be so important, the others do not matter (e.g., time available is so short, the act almost assuredly cannot be done regardless of the other factors). Further, if a specific situation warrants treatment of unique factors that are not, and cannot be

**Table 5-1 Post-Initiator PSFs To Be Considered**

<b>In-Control Room Actions</b>		<b>Ex-Control Room Actions</b>	
<b>Always Consider the Following PSFs</b>		<b>Always Consider the Following PSFs</b>	
Applicability and suitability of training and experience		Applicability and suitability of training and experience	
Suitability of relevant procedures and administrative controls		Suitability of relevant procedures and administrative controls	
Availability and clarity of instrumentation (cues to take actions as well as confirm expected plant response)		Availability and clarity of instrumentation (cues to take actions as well as confirm expected plant response)	
Time available and time required to complete the act, including the impact of concurrent and competing activities		Time available and time required to complete the act, including the impact of concurrent and competing activities	
Complexity of required response along with workload, time pressure, the need for special sequencing, and familiarity		Complexity of required response along with workload, time pressure, the need for special sequencing, and familiarity	
Team/crew dynamics and crew characteristics (degree of independence among individuals, operator attitudes - biases - rules, use of status checks, approach for implementing procedures, e.g., aggressive vs. slow and methodical...)			
Consideration of 'realistic' accident sequence diversions and deviations (e.g., extraneous alarms, failed instruments, outside discussions, sequence evolution not exactly like that trained on..) (Better Practice)			
<b>Additional PSFs to Consider</b>	<b>Conditions When Particularly Relevant</b>	<b>Additional PSFs to Consider</b>	<b>Conditions When Particularly Relevant</b>
Available staffing and resources	If typical CR staff is expected to be decreased or impacted so others must perform more than their typical tasks (not usually an issue)	Available staffing and resources	Particularly when many or complex actions need to occur concurrently or in a short time, and staffing needs may be stretched

<b>In-Control Room Actions</b>		<b>Ex-Control Room Actions</b>	
Human-machine interface	If could be problematic, or not easily accessed or used (not usually an issue but consider, for instance, the need to use backboards, deal with common workarounds...)	Human-machine interface	If could be problematic (e.g., poor labeling) or not easily accessed or used
<b>Additional PSFs to Consider</b>	<b>Conditions When Particularly Relevant</b>	<b>Additional PSFs to Consider</b>	<b>Conditions When Particularly Relevant</b>
Environment in which the act needs to be performed	Potentially adverse or threatening situations such as fire, flood, seismic, loss of ventilation...(not usually an issue)	Environment in which the act needs to be performed	Potentially adverse situations such as high radiation, high temperature, high humidity, smoke, toxic gas, noise, poor lighting, weather, flooding, seismic...
Accessibility and operability of equipment to be manipulated	If could be problematic, or not easily accessed or used such as the need to use backboards, or when indications/controls could be affected by the initiating event or other failures (e.g., loss of DC)	Accessibility and operability of equipment to be manipulated	If could be problematic, or not easily accessed or used such as when the equipment could be affected by the initiating event or the environment (e.g., fire, flood, weather)
The need for special tools (keys, ladders, hoses, clothing such as to enter a radiation area...)	Not usually an issue but consider, for instance, accessibility of keys for keylock switches	The need for special tools (keys, ladders, hoses, clothing such as to enter a radiation area...)	For situations where other than simple switch or similar type operations are necessary, or when needed to be able to access the equipment

<b>In-Control Room Actions</b>		<b>Ex-Control Room Actions</b>	
Communications (strategy and coordination) as well as whether one can be easily heard	Not usually an issue - simply ensure that communication strategy allows crisp direction and proper feedback; otherwise only in special situations such as needing to communicate with SCBAs on	Communications (strategy and coordination) as well as whether one can be easily heard	For situations where communication among crew members (locally and/or with CR) are likely to be needed and there could be a threat such as too much noise, failure of the communication equipment, availability and location issues associated with the communication equipment...
<b>Additional PSFs to Consider</b>	<b>Conditions When Particularly Relevant</b>	<b>Additional PSFs to Consider</b>	<b>Conditions When Particularly Relevant</b>
Time of day	Special sequences or events such as involving numerous failures where task workloads may be extremely high and preferred additional in-CR staffing needs may be difficult to obtain such as during graveyard shift (typically not an issue)	Time of day	Particularly when many or complex actions need to occur concurrently or in a short time, and staffing needs may be stretched such as during graveyard shift
		Special fitness needs	For special situations expected to involve the use of heavy or awkward tools/equipment, carrying hoses, climbing...
		Team/crew dynamics and crew characteristics (degree of independence among individuals, operator attitudes - biases - rules, use of status checks, approach for implementing procedures, e.g., aggressive vs. slow and methodical...)	To the extent that the timing and the appropriateness of the directions from the CR, and the subsequent carrying out of the ex-CR action(s) could be affected

In-Control Room Actions		Ex-Control Room Actions	
		Consideration of 'realistic' accident sequence diversions and deviations (e.g., extraneous alarms, outside discussions, sequence not exactly like that trained on...)	To the extent that these could affect the timing, specific directions, or successful performance of the ex-CR action(s)

addressed by the following list of factors, identification of other performance-shaping factors should complement the list below. Consideration of the impact of the factors on the HEPs should be as plant- and accident sequence-specific as necessary to address the issue and confirmed, where useful, by such techniques as talkthroughs, walkdowns, field observations, simulations, and examination of past events in order to be realistic. Appendix A provides more specific guidance and discussion of the PSFs presented below, as well as why some are considered generally more important than others.

It should be apparent that the factors seemingly most relevant to the act (either as positive or negative influences) and having the most impact on the HEP, have been considered quantitatively. Further, the more the impacts of the factors have been determined based on talkthroughs, walkdowns, field observations, and simulations vs. simple assumptions or judgements, the better the quality of the HEP evaluations.

#### 5.3.3.6 Good Practice #6:

Dependencies among the post-initiator HFES and hence the corresponding HEPs in an accident sequence should be quantitatively accounted for in the PRA model by virtue of the joint probability used for the HEPs. This is to account for the evaluation of each sequence holistically, considering the performance of the operators throughout the sequence response and recognizing that early operator successes or failures can influence later operator judgments and subsequent actions. This is particularly important so that too optimistic combined probabilities are not inadvertently assigned potentially resulting in the inappropriate decrease in the risk significance of human actions and related accident sequences and equipment failures. In the extreme, this could result in the inappropriate screening out of accident sequences from the model because the combined probability of occurrence of the events making up an accident sequence drops below a threshold value used in the PRA to drop sequences from the final risk results.

In analyzing for possible dependencies among the HFES in an accident sequence, look for links among the acts including:

- the same crew member(s) is responsible for the acts,
- the actions take place relatively close in time in the sense that a crew "mindset" or interpretation of the situation might carryover from one event to the next,

- the procedures and cues used along with the plant conditions related to performing the acts are identical (or nearly so) or related, and the applicable steps in the procedures have few or no other steps in between the applicable steps,
- there are similar performance shaping factors for performing the acts,
- how the acts are performed is similar and they are performed in or near the same location, and
- there is reason to believe that the decision processes associated with the events might be related and the interpretation of the need for one action might bear on the crews decision regarding another action.

The more the above commonalities and similarities exist, the greater the potential for dependence among the HFES (i.e., if the first act is not performed correctly, there is a higher likelihood the second, third... act(s) will also not be performed correctly; or vice versa if the act(s) are successful). For example, if nearly all or all of the above characteristics exist, very high or complete dependence should generally be assumed. If only one or two of the above characteristics exist, then analysts will need to evaluate the likely strength of their effect and the degree of dependence that should be assumed and addressed in quantification.

The resulting joint probability of the HEPs in an accident sequence should be such that it is in line with the above characteristics and the following guidance, unless justified otherwise:

- The total combined probability of all the HFES in the same accident sequence/cut set should not be less than a justified value. It is suggested that the value not be below the ~0.0001 to 0.00001 range since it is typically hard to defend that other not specifically treated dependent failure modes (e.g., even heart attack) cannot occur. Depending on the independent HFE values, the combined probability may need to be higher.
- To the extent the joint HEPs are looked at separately, but a previous human action in the sequence has failed, then:
  - ▶ A factor of 3-10 higher than what would have been the independent HEP value for the subsequent act(s) exists for low to moderate dependence
  - ▶ 0.1 up to 0.5 is the resulting probability value used for the subsequent HEP(s) for high dependence
  - ▶  $\geq 0.5$  exists for the subsequent HEP(s) for very high or 1.0 for complete dependence.

#### 5.3.3.7 Good Practice #7:

Mean values for each HEP (excluding conservative HEPs) and an assessment of the uncertainty in the mean values should be performed at least for the dominant HEPs to the extent that these uncertainties need to be understood and addressed in order to make appropriate risk-related decisions. Assessments of uncertainty are typically performed by:

- assigning uncertainty distributions for the HEPs and propagating them thru the quantitative analysis of the entire PRA such as by a Monte Carlo technique, and/or
- performing sensitivity analyses that demonstrate the effects on the risk results for extreme estimates in the HEPs based on at least the expected uncertainty range about the mean value.

Note, in some cases, it may be sufficient to address the uncertainties by just qualitative arguments without the need to specifically quantify them (e.g., justifying why the HEP cannot be very uncertain or why a change in the HEP has little relevancy to the risk-related decision to be made).

In assessing the uncertainties and particularly when assigning specific uncertainty distributions, the uncertainties should include (a) those epistemic uncertainties existing because of lack of knowledge of the true expected performance of the human for a given context and associated set of performance-shaping factors (i.e., those factors for which we do not have sufficient knowledge or understanding as to the “correct” HEP, such as how time of day affects the bio-rhythm and hence, performance of operators), and (b) consideration of the combined effect of the relevant aleatory (i.e., random) factors to the extent they are not specifically modeled in the PRA and to the extent that they could significantly alter the context and performance-shaping factor evaluations for the HFE, and thereby the overall HEP estimate.

Concerning the latter, while it is best to specifically model the aleatory factors in the PRA (i.e., those factors that are random and could significantly affect operator performance, for example, the time of day the initiator occurs, whether or not other nuisance alarms or equipment failures may co-exist with the more important failures in the sequence, whether a critical equipment failure occurs early in the sequence or late in the sequence, etc.), this is often impractical and is typically not done as it would make the PRA model excessively large and unwieldy. Thus in assigning the mean HEP and uncertainty distribution, analysts should reflect an additional contribution from random factors associated with the plant condition or overall action context. This can be done by considering the relevant aleatory (i.e., random) factors, their likelihoods of occurrence, and their effects on the HEP estimate.

For example, suppose for an accident sequence(s) it is judged that the human performance will be significantly affected by the number of “nuisance and extraneous failures,” as opposed to when no or few nuisance/extraneous failures exist (and yet these two plant “states” are not explicitly defined by the PRA model). Further, based on the analyst considering how the HEP is affected, a value of  $P_0$  would be estimated for when no or few nuisance/extraneous failures exist and a value of  $P_1$  would be estimated for when many do exist, and the difference between  $P_0$  and  $P_1$  is significant (e.g., factor of 10). It is also judged that many nuisance/extraneous failures will occur about 50% of the time based on past experience. The resulting combined mean HEP value is  $0.5P_0 + 0.5P_1$  considering this random factor. The overall uncertainty about the combined mean HEP value should reflect the weighted epistemic uncertainties in  $P_0$  and  $P_1$  (such as by a convolution approach, via an approximation, or other techniques). While it is not expected that such a detailed evaluation be done for every random situation or for every HEP, the mean and uncertainty estimates for the most dominant HEPs should account for any such perceived important aleatory factors that have not otherwise been accounted for (i.e., the factors, considering their likelihoods and effects on the HEP, are anticipated to have a significant impact on the resulting overall HEP).

Whatever uncertainty distributions are used, the shape of the distributions (log-normal, normal, beta...) are typically unimportant to the overall risk results (i.e., the PRA results are usually not sensitive to specific distributions). Further, typical uncertainties include values for the HEP that represent a factor of 10 to 100 or even more between the lower bound value and the upper bound value that encompass the mean value.

#### 5.3.3.8 Good Practice #8:

The post-initiator HEPs (excluding the conservative HEPs) should be reasonable from two standpoints:

- first and foremost, relative to each other (i.e., the probabilistic ranking of the failures when compared one to another), and
- in absolute terms (i.e., each HEP value) to the extent that the sensitivity of the risk-related decision is not important as to the absolute values for the HEPs.

This reasonableness should be checked based on consideration of actual plant experience and history, against other evaluations (such as for similar acts at other plants), and the qualitative understanding of the actions and the relevant contexts and performance-shaping factors under which the acts are performed.

It is suggested that a rank-ordered list of the post-initiator HFEs by probability be used as an aid for checking reasonableness. As part of such a list, it is particularly worthwhile to compare “like” HFEs for different sequences such as failure to manually depressurize in a BWR when all high pressure injection is lost during a LOCA as compared to the same action but during a simple transient. For example, simple, procedure-guided actions with easily recognized cues and plenty of time to perform the actions, should have lower HEPs than complex, memorized, short time available type actions, all other factors being the same. Typical expectations of most post-initiator HEPs are in the 0.1 to 0.0001 range and depend particularly on the relevant contextual factors and proper consideration of dependencies as discussed under many of the Good Practices covered above. Helpful checks include:

- For a HFE, do any one or two dominant performance-shaping factors exist or is the cumulative effect of the relevant performance-shaping factors such that they are either so negative or so positive that a ‘sanity check’ would suggest a high HEP (e.g., 0.1) or a low HEP (e.g., 1E-4) respectively? Accordingly, this very high or low probability HFE should be one of the higher or lower probability HFEs relative to the other HFEs in the model. For example, while the manual scram action may need to be done in a short time, it is a proceduralized action, is often an early step in procedures, is performed often in training, and thus has become such an “automatic” action (the predominant positive factor) that a low HEP is justified.
- Are there seemingly balanced combinations of both positive and negative factors, or are there weak to neutral factor effects? If so, this is likely to lead to in-between values for the HEPs (e.g., ~0.01) placing these HFEs (relative to others) ‘in the middle’.
- Do the individual HEPs and the relative ranking of the HFEs seem consistent with actual or simulated experience? For example, if it is known that operators ‘have trouble with’ a specific act(s) in simulations or practiced events, and yet the assigned HEP is very low (e.g., 1E-3 or

lower), this may be a reason to question and revisit the assigned HEP.

- Do other similar plant and action analyses support the HEP evaluation? Recognize, however, that there may be valid reasons why differences may exist and thus this check is not likely to be as helpful as the others above.

#### 5.3.4 POSSIBLE IMPACTS OF NOT PERFORMING GOOD PRACTICES AND ADDITIONAL REMARKS:

Besides the obvious concerns about inaccuracies in the HEP quantification and thus whether the HEPs “make sense”, as well as the resulting potential misinformation about the dominant risk contributors if quantification is not done well, the following observations are noted.

- Use of conservative values is a useful and most often, necessary part of HRA so as to avoid the expenditure of resources on unimportant human events and accident sequences. The above guidance is aimed at allowing some conservative values without inadvertently and inappropriately allowing the analytical phenomenon of, for instance, multiplying four human events in the same sequence each at a conservative estimate of  $1E-1$  to yield a  $1E-4$  combined probability, without checking for dependencies among the human events. In such a case some human failure events and combinations of events, or even whole accident sequences, may inappropriately screen out of the PRA model entirely because the accident sequence frequency drops below a model threshold. Hence some of the dominant individual or combination contributors may be missed. This is why the conservative estimates both individually and for combined events should not be too low. Further, if conservative values are left permanently assigned to some human failure events that should be assessed with more detail to obtain a more realistic assessment of risk (supposedly lowering the probability), the risk significance of these human failure events and related equipment failures are likely to be over-emphasized at the expense of improperly lessening the relative importance of other events and failures.
- It is important to be sure that dependencies among the various modeled HFEs including those with conservative values, have been investigated. Treating HFEs, whether with conservative values or based on more detailed analysis, as independent acts without checking for dependencies (thereby being able to multiply the individual HEPs) can inappropriately lessen the risk significance of those HFEs and related equipment failures in accident sequences. This can cause the inappropriate dropping out of accident sequences because the sequences quantitatively drop below a model threshold value as discussed above under screening. Proper consideration of the dependencies among the human actions in the model is necessary to reach the best possible evaluation of both the relative and absolute importance of the human events and related accident sequence equipment failures.
- The use of mean values and addressing uncertainties are a part of the Regulatory Guide 1.174<sup>11</sup> guidance and to the extent addressed therein, the HRA quantification needs to be consistent with that guidance when making risk-informed decisions.
- There can be a tendency for analysts to want to use an existing PRA model to address issues such as changes to the plant, without spending the appropriate time to revisit some of the underlying assumptions and modeling choices made to create the original PRA. A review should be done to

see if these assumptions and choices still apply for the issue being addressed. In this case, some post-initiator human failure events may be quantified in the original model using conservative estimates and detailed failure probabilities that may not be appropriate for the new issue being addressed. As an example, where higher conservative values may have been acceptable for purposes of the original PRA, these may over-estimate the contribution of these human failure events for the issue being addressed. Further, the relative risk contribution of equipment and associated accident sequences with which the human failure events appear, may be artificially too high (and therefore other events too low) because of the conservative values. Hence it is good practice to revisit the use of conservative estimates and detailed human failure event probabilities in order to appropriately address the issue.

## **5.4 Adding recovery actions to the PRA**

5.4.1 **OBJECTIVE:** To address what recovery actions can be credited in the post-initiator HRA and the requirements that should be met before crediting recovery actions. Adding recovery actions is common practice in PRA and accounts for other reasonable actions the operators might take to avoid severe core damage and/or a large early release that are not already specifically modeled. For example, in the PRA modeling of an accident sequence involving a loss of offsite power, subsequent station blackout, and loss of all injection, it would be logical and common to credit the operators attempting to recover offsite or onsite power (and thus ac-powered core cooling systems) as well as perhaps locally aligning an independent firewater system (not affected by the station blackout) for injection. The failure to successfully perform such actions would subsequently be added to the accident sequence model thereby crediting the actions and further lowering the overall accident sequence frequency because it takes additional failure of these actions before the core is actually damaged. The following provides good practices for crediting post-initiator recovery actions while implementing the related Standard requirements.

### **5.4.2 CORRESPONDING ASME STANDARD REQUIREMENTS:**

The Standard requires that recovery actions be modeled only if it has been demonstrated that the action is plausible and feasible for those sequences to which they are applied. There are multiple supporting requirements in the Standard that address what recovery actions can be credited as well as the need to consider dependencies among the HFEs and any recovery actions that are credited.

### **5.4.3 GOOD PRACTICES:**

#### **5.4.3.1 Good Practice #1:**

Based on the failed functions, systems, or components, identify recovery actions to be credited that are not already included in the PRA (e.g., restoring offsite power loss, aligning another backup system not already accounted for...) and that are appropriate to be tried by the crew to restore the failure. The following should be considered in defining appropriate recovery actions:

- the failure to be recovered,
- whether the cues will be clear and provided in time to indicate the need for a recovery action, and the failure that needs to be recovered,
- the most logical recovery actions for the failure and based on the cues that will be provided,
- the recovery is not a repair action (e.g., the replacement of a motor on a valve so that it can be operated),
- whether sufficient time is available following the timing of the cues (for the sequence/cut set) for the recovery action to be diagnosed and implemented to avoid the undesired outcome,
- whether sufficient crew resources exist to perform the recovery(ies),
- whether there is procedure guidance to perform the recovery(ies),
- whether the crew has trained on the recovery action(s) including the quality and frequency of the training,
- whether the equipment needed to perform the recovery(ies) is accessible and in a non-threatening environment (e.g., extreme radiation), and
- whether the equipment needed to perform the recovery(ies) is available in the context of other failures and the initiator for the sequence/cut set.

In addressing the above issues and assessing which recovery action, or a few, to credit in the PRA, just as with any other HFE, all the good practices provided earlier in Sections 5.1, 5.2, and 5.3 apply to these recovery actions as well (i.e., the failure to recover is just another HFE like all the other post-initiator HFEs). In general, no recovery should be credited where any of the above considerations are not met (e.g., there is not sufficient time, there are no cues that there is a problem, there are not sufficient resources, there is no procedure or training, etc.). Exceptions may be able to be justified in unique situations, such as a procedure is not needed because the recovery is a skill-of-the-craft, non-complex, and easily performed; or the specific failure mode of the equipment is known for the sequence (this is usually not the case at the typical level of detail in a PRA) and so “repair” of the failure can be credited because it can be easily and quickly diagnosed and implemented. Any exceptions should be documented as to the appropriateness of the recovery action.

When considering multiple recoveries (i.e., how many recoveries to be credited in one accident sequence/cut set), the above considerations apply to all the recoveries. The analyst should also consider that one recovery may be tried (perhaps even multiple times) and then the second recovery may be tried but with even less time and resources available because of the attempts on the first recovery. Hence the failure probability of the second recovery should be based on more pessimistic characteristics (e.g., less time available, less resources, etc.) than if such a possibility is not considered.

#### 5.4.3.2 Good Practice #2:

As stated above, all the good practices provided earlier in Sections 5.1, 5.2, and 5.3 apply. From these good practices, particular attention should be paid to accounting for dependencies among the HFEs including the credited recovery actions. More specifically, dependencies should be assessed:

- among multiple recoveries in the accident sequence/cut set being evaluated, and
- between each recovery and the other HFEs in the sequence/cut set being evaluated..

As part of this effort, the analyst should give proper consideration to the difficulties people often have in overcoming an initial mind-set despite new evidence (e.g., look how long the PORV remained open in the Three Mile Island accident despite new cues of the problem, different personnel, etc.). For this and similar reasons, the assessing of no dependence needs to be adequately justified to ensure the quantified credit for the recovery action(s) is not unduly optimistic.

#### 5.4.3.3 Good Practice #3:

Quantify the probability of failing to perform the recovery(ies) by:

- using representative data that exists and deemed appropriate for the recovery event (i.e., a data-based approach such as using data that exists for typical times to recover offsite power)
- using the HRA method/tool(s) used for the other HFEs (i.e., using an analytical/modeling approach).

In performing the quantification, one should ensure that all the good practices under Section 5.3 are followed (for each individual recovery as well as for multiple/joint recovery credit). In addition, if using data, ensure the data is applicable for the plant/sequence context or that the data is modified accordingly. For example, a plant may use available experience data for the probability of failing to align a firewater system for injection but the experience data is based on designs for which all the actions can be taken from the main control room whereas for this plant, the actions have to be performed locally.

#### 5.4.4 POSSIBLE IMPACTS OF NOT PERFORMING GOOD PRACTICES AND ADDITIONAL REMARKS:

The primary concern for not performing the above good practices is that recovery credit could be applied too optimistically; that is, the failure to recover is assigned too low a probability. Hence an under-estimate of the failure to recover is applied to the PRA accident sequence/cut set, making the affected sequence/cut set artificially too low in risk significance. This can subsequently affect the ranking of the important sequences, equipment failures, and human actions potentially leading to false conclusions of the dominant risk contributors.

## 6. HRA DOCUMENTATION

The ASME Standard<sup>5</sup> provides a set of requirements for documenting a human reliability analysis (HRA) in a manner that facilitates PRA applications, upgrades, and peer review. Specific requirements are provided. The following provides good practice for documenting a HRA building on those requirements.

### Good Practice:

The level of detail that needs to be addressed in the documentation is dependent on the PRA application and the issue being addressed as well as the objectives, scope, and level of detail of the analysis. Whatever documentation is provided, the test for adequate documentation should be: “Can a knowledgeable reviewer understand the analysis to the point that it can be at least approximately reproduced and the resulting conclusion reached if the same methods, tools, data, key assumptions, and key judgments and justifications are used?” Hence, the documentation should include the following, but only to the extent it is applicable for the application:

- the overall approach and disciplines involved in performing the HRA including to what extent talk-throughs, walkdowns, field observations, and simulations were used,
- summary descriptions of the HRA methodologies, processes, and tools used to:
  - ▶ identify the pre-and post-initiator human actions,
  - ▶ screen pre-initiators from modeling,
  - ▶ model the specific HFEs including decisions about level of detail and the grouping of individual failures into higher order HFEs,
  - ▶ quantify the HEPs with particular attention to the extent to which plant and accident sequence-specific information was used, as well as how dependencies were identified and treated,
- assumptions and judgments made in the HRA, their bases, and their impact on the results and conclusions (generic or on a HFE-specific basis, as appropriate),
- for at least each of the HFEs important to the risk decision to be made, the PSFs considered, the bases for their inclusion, and how they were used to quantify the HEPs, along with how dependencies among the HFEs and joint probabilities were quantified,
- the sources of data and related bases or justifications for:
  - ▶ the screening and conservative values,
  - ▶ the best estimate values and their uncertainties with related bases,
- the results of the HRA including a list of the important HFEs and their HEPs, and
- conclusions of the HRA.

## 7. ERRORS OF COMMISSION (EOCs)

Explicit modeling of errors of commission (i.e., committing an incorrect act) has generally been beyond current PRA practice and is not explicitly addressed in the ASME Standard HRA requirements. This is largely because practitioners believe that there is potentially a large number of acts that an operator might perform that are adverse to safe shutdown (i.e., fail or make unavailable equipment/functions relevant to mitigating the scenario, or otherwise exacerbate the scenario such as opening a PORV and causing an unwanted loss of coolant accident) even for what may appear to be justifiable reasons. Errors of omission (i.e., failure to perform the correct act) are typically modeled in PRAs because the set of correct acts is better known for each sequence, thus limiting the number of human failures that need to be modeled. At best, PRAs have handled EOCs implicitly (e.g., as part of a base HEP) without a systematic or adequate search for this type of error.

However, more recent methods (e.g., ATHEANA) are making advances in the ability to identify EOCs without the need of performing an exhaustive search. One of the lessons learned from the development and application of ATHEANA is that the effort needed to identify EOCs can be substantially reduced by focusing the search on identifying systematic vulnerabilities in plant operations associated with plant critical functions.

Given these advances and the potential for regulatory requirements to make the need to address EOCs more important, it is recommended that future HRA/PRAs attempt to identify and model potentially important EOCs. At a minimum, the use of risk in any issue assessment should at least ensure that conditions that promote likely EOCs do not exist, e.g., that such conditions have not been introduced by a plant change or modification. To the extent any EOCs are modeled, all the guidance in this document has been written with both types of errors in mind; that is, all the same good practices apply whether the error is one of omission or commission.

When considering the potential for situations that may make EOCs somewhat likely, the premise of any evaluation should be that:

- operators are performing in a rationale manner (e.g., no sabotage), and
- the procedural and training guidance is being used by the crew based on the plant status inputs they are receiving.

Using this premise, EOCs are considered to be largely the result of problems in the plant information/operating crew interface (wrong, inadequate information is present, or the information can be easily misinterpreted) or in the procedure-training/operating crew interface (procedures/training do not cover, very well, the actual plant situation because they provide ambiguous guidance, no guidance, or even unsafe guidance for the actual situation that may have evolved in a somewhat unexpected way).

With a present focus on reviewing potential applications of current PRAs, the following is offered as guidance in this area to aid in ensuring EOC-prone conditions do not exist or have not been introduced as part of a plant change. Hence, a review of a plant change should look for situations where one or

more of the following characteristics are introduced as a result of the change and thus should be corrected if possible.

- To deal with the ‘bad information’ interface, an analysis/review should at least look for those acts that operators may take that (a) would fail or otherwise make unavailable a PRA function or system, or (b) would reduce the accident mitigating redundancy available, or (c) would exacerbate an accident challenge, because the change has caused such an action to be performed on the basis of just one primary input/indication for which there is no redundant means to verify the true plant status. Such a situation identifies a vulnerable case where EOCs may likely be performed based on just one erroneous (failed, spurious, etc.) input such as an alarm, indicator, or verbal cue of an observed condition.

In identifying such cases, one should keep in mind that multiple indications may use the same faulty input (e.g., subcooling margin indication and primary system indication may use the same pressure transmitter(s); multiple reactor vessel level indications may rely on the same power supply) and hence a single fault may actually affect multiple inputs observable to the operator. Depending on the how the failure affects the indications (fail high, low, mid-scale, etc.), the failure may not be “obvious” and a EOC-prone situation may exist that may need to be rectified.

- To deal with the procedure-training interface, an analysis/review should at least look for those acts that operators may take that (a) would fail a PRA function or system, or (b) would reduce the accident mitigating redundancy available, or (c) would exacerbate an accident challenge, because the change has caused the procedure (including entry conditions) and/or training guidance:
  - ▶ to become ambiguous/unclear (e.g., vague criteria as to when to abandon the main control room),
  - ▶ to introduce a repetitive situation in the response steps where a way to proceed out of the procedure and/or the specific repetitive steps is not evident (e.g., at the end of a series of steps, the procedure calls for a return to a previous step with no clear indication as to how the operators ultimately get out of the repetitive loop of steps,
  - ▶ to place the operators in dilemma conditions without some guidance/criteria as to how to “solve” the dilemma (e.g., being vague as to whether or not to shutdown a diesel with a cooling malfunction when all other ac power is unavailable),
  - ▶ to require the operators to rely on memory especially for complex or multi-step tasks, or
  - ▶ to require the operators to perform calculations or make other manual adjustments especially in time-sensitive situations.

The above identify vulnerable cases where EOCs may likely be performed because the procedures and/or training do not adequately cover accident situations that may be faced by the operator or rely on techniques (require memory or adjustments) that may be difficult to perform properly especially when in a dynamic response situation. In these cases, mismatches between the actual event response

that is required and the procedure/training guidance can become magnified making conditions potentially more prone to EOCs.

DRAFT

## 8. REFERENCES

- [1] *Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement*, Federal Register, Vol 60, p. 42622 (60FR 42622), US Nuclear Regulatory Commission, August 16, 1995.
- [2] *Code of Federal Regulations 10, Parts 1 to 50*, Office of the Federal Register National Archives and Records Administration, Revised as of January 1, 2001.
- [3] *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis*, Regulatory Guide 1.174, Rev. 1, US Nuclear Regulatory Commission, November 2002.
- [4] *An Approach for Determining The Technical Adequacy of Probabilistic Risk Assessment Results For Risk- Informed Activities*, Draft Regulatory Guide 1.200, U.S. Nuclear Regulatory Commission, February 2004.
- [5] *Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications*, ASME RA-S-2002, American Society of Mechanical Engineers, April 5, 2002.
- [6] *Probabilistic Risk Assessment Peer Review Process Guidance*, NEI 00-02 Revision A3, Nuclear Energy Institute, March 2000
- [7] *Use of Probabilistic Risk Assessment in Plant-Specific, Risk-Informed Decisionmaking: General Guidance*, NUREG-0800, Chapter 19, Rev. 1, US Nuclear Regulatory Commission, November 2002.
- [8] A.D. Swain and H.E. Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications - Final Report*, NUREG/CR-1278, SAND80-0200, Sandia National Laboratories, August 1983.
- [9] Embrey, D. E., et al., *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.
- [10] *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)*, NUREG-1624, Rev. 1, US Nuclear Regulatory Commission, May 2000.
- [11] *Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants*, NUREG-1150, US Nuclear Regulatory Commission, December 1990
- [12] Alan D. Swain, *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772, SAND86-1996, Sandia National Laboratories, February 1987.

[13] *SHARPI - A Revised Systematic Human Action Reliability Procedure*, EPRI NP-7183-SL, Electric Power Research Institute, December 1990.

[14] *SPAR-H Method*, NUREG/CR- later, INEEL/EXT-02-10307, Idaho National Engineering and Environmental Laboratory, DRAFT, November 2002.

[15] J. Reason, *Human Error*, Cambridge, England: Cambridge University Press, 1990 and *Managing the Risks of Organizational Accidents*, Aldershot, UK: Ashgate, 1997.

[16] D.D. Woods et. al., *Behind Human Error: Cognitive Systems, Computers, and Hindsight*, Crew System Ergonomics Information Analysis Center (CSERIAC), The Ohio State University, Wright-Patterson Air Force Base, Columbus, OH, December 1994.

[17] M.R. Endsley, *Towards a theory of situation awareness in dynamic systems*, *Human Factors*, 37, pp. 65-84, 1995.

#### ACKNOWLEDGMENTS

We would like to thank Gareth Parry and Susan Cooper of the USNRC for several thorough reviews of this document at various stages of its development and for many important comments and suggestions. Similarly, we would like to thank Dennis Bley of Buttonwood Consulting and Bruce Hallbert of INEEL for their reviews and comments.

## APPENDIX A

### Guidance on Consideration of Performance-Shaping Factors for Post-Initiator HFEs

The following provides more detail on the performance-shaping factors presented in Section 5.3.3.5, including some key characteristics to consider when assessing the influence of these performance-shaping factors on the failure probability for a human failure event (HFE). Included are important interactions among the factors that should also be examined when assessing the holistic impact of the performance-shaping factors on operator performance. These factors need to be assessed on a plant-specific and accident sequence-specific basis considering the relevant context and the act to be performed.

It is important to re-iterate that this Appendix is written for the specific purpose of addressing post-initiator HFEs in a risk assessment for commercial nuclear power plant operations occurring nominally at full power, and for internal initiating events. However, much of it is considered useful to other modes of operation and for other industry applications such as safety assessments of chemical plants, space mission risk assessments, and others. Similarly, much of it is considered applicable for external initiating events but it should be used with the additional context of such events in mind (e.g., shaking during a seismic event). Additionally, portions of this Appendix may be of benefit in examining human actions related to nuclear materials and safeguard types of applications.

Specific HRA methods and tools used by the industry may define and “measure” these performance-shaping factors somewhat differently than described here. That is, they may use a different explicit set of performance-shaping factors that ‘roll-up’ many of the factors listed below into the definitions of their specific factors (e.g., stress, workload). Nevertheless, these summaries are provided as one means with which to assess that the specific HRA method/tool has been used such that the characteristics described here have indeed been accounted for in the evaluation of post-initiator human error probabilities (HEPs).

While quantitative guidance is not provided (specific quantification depends on the method/tool that is used), the following should be useful in arriving at whether a performance-shaping factor, regardless of the method/tool, qualitatively is a weak/strong positive, neutral (or not applicable), or negative influence. The method/tool that is used, should have established scales and corresponding definitions for assessing each PSF qualitatively (e.g., “good”, “adequate”, “poor”) and a way to interpret the result into a quantified HEP.

The performance-shaping factors are addressed below.

Applicability and suitability of training/experience. For both in-control room and local actions, this is an important factor in assessing operator performance. For the most part, in nuclear plants, operators can be considered “trained at some minimum level” to perform their desired tasks.

However, from a HRA perspective, the degree of familiarity with the type of sequences modeled in the PRA and the actions to be performed, can provide a negative or positive influence that should be assessed on the likelihood of operator success. In cases where the type of PRA sequence being

examined or the actions to be taken are not periodically addressed in training (such as covered in classroom sessions or simulated every one to two years or even more often) or the actions are not performed as part of their normal experience or on-job duties, this factor should be treated as a negative influence. The converse would result in a positive influence on overall operator performance.

One should also attempt to identify systematic training biases that may affect operator performance either positively or negatively. For example, training guidance in a pressurized water reactor (PWR) may provide a reluctance to use “feed and bleed” in a situation where steam generator feed is expected to be recovered. Other biases may suggest operators are allowed to take certain actions before the procedural steps calling for those actions are reached, if the operators are sure the actions are needed. Such training “biases” could cause hesitation and hence higher HEPs for the desired actions, as in the first case above, or as in the case of not waiting to take obvious actions, be a positive influence.

It is incumbent on the analyst to ensure that training and/or experience is relevant to the PRA sequence situation and desired actions. The more it can be argued that the training is current, “is like the real event,” is varied enough to represent differences in the way the event can evolve, and proficiency is demonstrated on a periodic basis, the more positive this factor. If there is little or no training/experience or there are potentially negative training biases for the PRA sequence being examined, this factor should be considered to have a negative influence.

Suitability of relevant procedures and administrative controls. For both in-control room and local actions, this is an important factor in assessing operator performance. Similar to training, for the most part, procedures exist to cover many types of sequences and operator actions.

However, from a HRA perspective, the degree the procedures clearly and unambiguously address the types of sequences modeled in the PRA and the actions to be performed, dictates whether they are a negative or positive influence on operator performance. Where procedures have characteristics like those below related to the desired actions for the sequences of interest, this factor should be considered a negative influence:

- ambiguous/unclear/non-detailed steps for the desired actions in the context of the sequence of interest,
- situations can exist where the operators are likely to have trouble identifying a way to proceed forward,
- there is a requirement to rely on considerable memory,
- operators must perform calculations or make other manual adjustments especially in time-sensitive situations,
- there is no procedure or the procedure is likely to not be available especially when taking local actions “in the heat of the scenario” and it cannot be argued that the desired task is simple and a “skill of the craft” or automatic/memorized activity that is trained on or there is routine experience.

Otherwise, this factor should be considered as adequate or even a positive influence.

Talk-throughs with operations and training staff can be helpful in uncovering ‘difficulties’ or ‘ease’ in using the relevant procedures considering the associated training that the operators receive and the way the operators interpret the use of the procedures.

Availability and clarity of instrumentation (cues to take actions as well as confirm expected plant response). For both in-control room and local actions, this is an important factor since operators, other than for immediate and memorized response actions, take actions based on diagnostic indications and look for expected plant responses to dictate follow-on actions. For in-control room situations, typical nuclear plant control rooms have sufficient redundancy and diversity for most important plant parameters. For this reason, most HRA methods inherently assume that adequate instrumentation typically exists. Nevertheless, this should be verified looking for the following characteristics that could make this a negative performance-shaping factor, particularly in situations where there is little redundancy in the instrumentation associated with the act(s) of interest:

- the key instrumentation associated with an act is adversely affected by the initiating event or subsequent equipment failure (e.g., loss of DC power causing loss of some indications, spurious or failed as a result of a hot short from a fire)
- the key instrumentation is not readily available and may not be typically scanned such as on an obscure back panel
- the instrumentation could be misunderstood or may be ambiguous because it is not a direct indication of the equipment status (e.g., PORV position is really the position of the solenoid valve and not the PORV itself)
- the instrumentation is operating under conditions for which it is not appropriate (e.g., calibrated for normal power conditions as opposed to shutdown conditions)
- there are so many simultaneous changing indications and alarms or the indication is so subtle, particularly when the time to act is short, it may be difficult to “see and pick out” the important cue in time (e.g., a changing open-close light for a valve without a concurrent alarm or other indication, finding one alarm light among hundreds).

The above also applies to local actions outside the control room, recognizing that in some situations, less instrumentation may exist (e.g., only one division of instrumentation and limited device actuators on the remote shutdown panel). However, on the positive side, local action indications often can include actual/physical observation of the equipment (e.g., pump is running, valve stem shows it is closed) that compensates for any lack of other indicators or alarms.

It is incumbent on the analyst to ensure that adequate instrumentation is available and clear so that the operators will know the status of the plant and when certain actions need to be taken.

Time available and time required to complete the act, including the impact of concurrent and

competing activities. This can be an important influence for both in-control room and local actions since clearly, if there is not enough or barely enough time to act, the estimated HEP is expected to be quite high. Conversely, if the time available far exceeds the time required and there are not multiple competing tasks, the estimated HEP is not expected to be strongly influenced by this factor.

It is important that the time available and the time needed to perform the act be considered *in concert with* many of the other performance-shaping factors and the demands of the sequence. This is because the thermal-hydraulic inputs (e.g., time to steam generator dryout, time to start uncovering the core), while important, are not the only influences. (Note, it is best if the thermal-hydraulic influences are derived from plant-specific or similar analyses rather than simple judgments).

The time to perform the act, in particular, is a function of the number of available staff, the clarity and repetitiveness of the cues that the act needs to be performed, the HMI, the complexity involved (discussed later), the need to get special tools or clothing (discussed later), consideration of diversions and other concurrent requirements (discussed later), where in the procedures the steps for the act of interest are called out, crew characteristics such as whether the crews are generally aggressive or slow and methodical in getting through the procedural steps, and other potential ‘time sinks’.

Clearly there is judgment involved, but as described here, it is not as simple as watching an operator perform an act in ideal conditions with a stop watch to determine the time required to perform the act. Only when the sequence context is considered holistically with the interfacing performance-shaping factors that have been mentioned here, can more meaningful “times” be estimated. Hence, especially for complex acts and/or situations, walkdowns and simulations can be helpful in ensuring overly optimistic “times” have not been estimated. Whatever HRA method/tool is used, determination of these times should include the considerations provided here.

Complexity of required response along with workload, time pressure, the need for special sequencing, and the familiarity of the situation. This is one of those catch-all type factors that attempts to measure the overall complexity involved for the situation at hand and for the act itself (e.g., many steps have to be performed by the same operator in rapid succession vs. one simple skill-of-the craft action). Many of the other performance-shaping factors address elements of the overall complexity such as the need to decipher numerous indications and alarms, many and complicated steps in a procedure, poor HMI, etc. Nevertheless, this factor should also capture ‘measures’ such as the ambiguity of the task, the degree of mental effort or knowledge involved, whether this is a multi-variable or single variable associated task, the overall task load and time pressure on the operators, whether special sequencing is required in order for the act to be successful especially if it involves multiple persons in different locations, whether the activity may require very sensitive and careful manipulations by the operator, etc. The more these “measures” describe an overall complex situation, this performance-shaping factor should be found to be a negative influence. To the extent these “measures” suggest a simple, straightforward, unambiguous process, this factor should be found to be nominal or even ideal (i.e., positive influence).

Team/crew dynamics and crew characteristics (degree of independence among individuals, operator attitudes - biases - rules, use of status checks, approach for implementing procedures, e.g., aggressive vs. slow and methodical crew). This is another catch-all type of factor which can be important

particularly to in-control room actions where the early responses to an event occur and the overall strategy for dealing with the event develops. In particular, the way the procedures are written and what is (or is not) emphasized in training (may be related to an organization influence), can cause systematic and nearly homogeneous biases and attitudes in most or all the crews that can affect overall crew performance. A review of this factor should include looking for such characteristics as:

- are independent actions encouraged or discouraged among crew members (allowing independent actions may shorten response time but could cause inappropriate actions going unnoticed until much later in the scenario)
- are there common biases or 'informal rules' such as a reluctance to do certain acts, whether the overall philosophy is to protect equipment or run it to destruction if necessary, or the way procedural steps are interpreted
- are periodic status checks performed (or not) by most crews so that everyone has a chance to 'get on the same page' and allow for checking what has been performed to ensure the desired activities have taken place
- is the overall approach of most crews to aggressively respond to the event, including taking allowed shortcuts through the procedural steps (which will shorten response times), or are typical responses slow and methodical (we trust the procedures type of attitude) thereby tending to slow down response times but making it less likely to make mistakes.

Observing simulations and using talk-throughs and walkdowns can provide valuable insights into the overall crew response dynamics, attitudes, and the typical times it takes them to get through various procedure steps and deal with unexpected failures or distractions. This knowledge can be a key input into the HEP evaluation including determining the typical time to respond (see that factor above).

Consideration of 'realistic' accident sequence diversions and deviations (e.g., extraneous alarms, outside discussions, the sequence evolution is not exactly like that trained on...). Particularly for in-control room actions where the early responses to an event occur and the overall strategy for dealing with the event develops, this can be an important factor to be considered. Through simulations, training, and the way the procedures are written, operators 'build up' some sense of expectations as to how various types of sequences are likely to proceed; even to the extent of recognizing alarm and indication patterns and what actions will likely be appropriate. To the extent the actual sequence may not be 'just like in the simulator,' such as involving other unimportant or spurious alarms, the need for outside discussions with other staff or even offsite entities such as a fire department, differences in the timing of the failed events, and behavior of critical parameters, etc., all can add to the potential diversions and distractions that may delay response timing or in the extreme, even confuse the operators as to the appropriate actions to take.

Hence the 'signature' of the PRA accident sequence and the potential acts of interest should be examined against the expectations of the operators to determine if there is a considerable potential for such distractions and deviations. Observing simulations and talking with the operators can help in discovering such possibilities. This could impact the HEP mean value estimate as well as the

uncertainty in the HEP, which may be important to assessing the potential risk or in establishing the limits for doing sensitivity studies with the HEP.

Available staffing/resources. For in-control room actions, this is generally not an important consideration (i.e., not a particularly positive or negative factor) since plants are supposed to maintain an assigned minimum crew with the appropriate qualified staff available in or very near the control room.

However, for ex-control room local actions, this can be an important consideration particularly dependent on (a) the number and locations of the necessary actions, (b) the overall complexity of the actions that are required to be taken, and (c) the time available to take the actions and the time required to perform the actions (see above for more on these related factors). For instance, where the number of actions are few and complexity is low and time available is high, one or two personnel available to perform the local actions may be more than enough and thus the available staffing can be considered to be adequate or even a positive factor. On the other hand, where the number of actions and their complexity is high, and with little time, perhaps three or more staff may be necessary. Additionally, the time of the day the initiating event occurs may be a factor since typically, night and graveyard shifts have fewer people available than the day shift (see more on this particular factor, below).

It is incumbent on the analyst to demonstrate that the available staffing is sufficient to perform the desired actions and/or assess the HEP(s) accordingly.

Human-machine interface (HMI). This is generally not an important factor relative to in-control actions since, given the many control room design reviews and improvements and the daily familiarity of the control room boards and layout, problematic human-machine interfaces have been taken care of or are easily worked around by the operating crew. Of course, any known very poor human-machine interface should be considered as a negative influence for an applicable action even in the control room. For example, if common workarounds are known to exist that may negatively influence a desired act, this should be accounted for in the HEP evaluation. Furthermore, it is possible that some unique situations may render certain human-machine interfaces less appropriate and for such sequences, the relevant interfaces should be examined.

However, since local actions may involve more varied (and not particularly human-factored) layouts and require operators to take actions in much less familiar surroundings and situations, any problematic human-machine interfaces can be an important negative factor on operator success. For instance, if to reach a valve to open it manually requires the operator to climb over pipes and turn the valve with a tool while in a laid out position, or in-field labeling of equipment is generally in poor condition and could lengthen the time to find the equipment, etc., such 'less ideal' human-machine interfaces could mean this is a negative performance-shaping factor. Otherwise, if a review reveals no such problematic interfaces for the act(s) of interest, this influence can be considered adequate or even positive.

Walkdowns and field or simulator observations can be useful tools in discovering problems (if any exist) in the human-machine interface for the actions of interest. Sometimes, discussions with the operators will reveal their own concerns about issues in this area.

Environment in which the act needs to be performed. Except for relatively rare situations, this factor is not particularly relevant to in-control room actions given the habitability control of such rooms and the rare challenges to that habitability (e.g., control room fire, loss of control room ventilation, less lighting as a result of station blackout). However, for local actions, this could be an important influence on the operator performance. Radiation, lighting, temperature, humidity, noise level, smoke, toxic gas, even weather for outside activities (e.g., having to go on a potential snow-covered roof to reach the atmospheric dump valve isolation valve), etc., can be varied and far less than ideal. Hence any HEP assessment should ensure that the influence of the environment where the act(s) needs to take place is accounted for as a performance-shaping factor. This factor may be non-problematic (adequate) or a negative influence (even to the point of not being able to perform the act).

Accessibility and operability of the equipment to be manipulated. As with the environment factor, this factor is not particularly relevant most of the time to in-control room actions except for special circumstances such as loss of operability of indications or controls as a result of the initiator or equipment failures (e.g., loss of DC). However, for local actions, accessibility and the operability of the equipment to be manipulated may not always be ensured, and needs to be assessed in the context with such influences as the environment, the need to use special equipment (discussed later), and HMI. Hence any HEP assessment should ensure that this factor, for where the act(s) needs to take place, is accounted for as a performance-shaping factor. This factor may be non-problematic (adequate) or a negative influence (even to the point of not being able to perform the act).

The need for special tools (keys, ladders, hoses, clothing such as to enter a radiation area...). As for the environment and accessibility factors, this factor is not particularly relevant to in-control room actions with the common exception of needing keys to manipulate certain control board switches or similar controls (e.g., key for explosive valves for standby liquid control injection in a BWR). However, for local actions, such needs may be more commonplace and necessary in order to successfully perform the desired act. If such equipment is needed, it should be ensured that the equipment is readily available, its location is readily known, and it is either easy to use or periodic training is provided, in order for this factor to be considered to be positive or adequate. Otherwise, this factor should be considered to have a negative influence on the operator performance, perhaps even to the point of making the failure of the desired action very high.

Communications (strategy and coordination) as well as whether one can be easily heard). For in-control room actions, this factor is not particularly relevant although there should be verification that the strategy for communicating in the control room is one that tends to ensure that directives are not easily misunderstood (e.g., it is required that the board operator repeat the act to be performed and then wait for confirmation before taking the act). Generally, it is expected that this will not be problematic; but any potential problems in this area (such as having to talk with special air packs and masks on in the control room in a minor fire) should be accounted for if they exist.

For local actions, this factor may be much more important because of the possible less than ideal environment or situation. It should be assured that the initiating event (e.g., loss of power, fire, seismic) or subsequent equipment faults are not likely to negatively affect the ability for operators to communicate as necessary to perform the desired act(s). For instance, having to set-up the equipment

and talk over significant background noise and possibly having to repeat oneself many times should be a consideration - even if just as a possible 'time sink' for the time to perform the act. Additionally, there should be training on the use of the communication equipment, its location is readily known, and its operability periodically demonstrated and shown to be in good working condition. Depending on the status of these characteristics, this factor may be non-problematic (adequate) or a negative influence (even to the point of not being able to perform the act).

Special fitness needs: While typically not an issue for in-control room actions, this could be an important factor for a few local actions depending on the specific activity involved. Having to climb up or over equipment to reach a device, needing to move and connect hoses, using an especially heavy or awkward tool, are examples of where this factor could have some influence on the operator performance. In particular, the response time for an action may be increased for successful performance of the act. Physically demanding (or not) activities should be considered in the evaluation of any HEP where it is appropriate to do so. Talk-throughs or field observations of the activities involved can help determine whether such issues are relevant to a particular HFE.

Time of day: While it is recognized that time of day and similar influences such as day of shift can affect the bio-rhythm of personnel and potentially their performance, not much is understood on how to quantify such effects. Moreover, it is typically the PRA's intent to measure an average risk for the whole year, as opposed to at a specific point in time. For these reasons, time of day is not typically specifically treated in a HEP evaluation.

However, at least one easily measurable effect of the time of day is on the available level of staffing during the early stages of a transient response (see available staffing factor above). Especially if there are significant differences in the staffing levels depending on the time of day, it is advisable to either treat the staffing level in a HEP evaluation as the minimum available depending on the shift, or probabilistically account for these aleatory differences more explicitly in the PRA model.