USE OF MINIMUM BOUNDS FOR JOINT HUMAN ERROR PROBABILITIES IN PRA

Mary Presley[1], Gareth Parry[2], Jeff Julius[3], Kaydee (Kohlhepp) Gunter[3], Jan Grobbelaar[3], Michael Hirt[3]

[1] *Electric Power Research Institute [EPRI]: 1300 W WT Harris Blvd., Charlotte, NC 28213, mpresley@epri.com*
[2] *Jensen Hughes: 2175 N. Main St., Suite 510, Walnut Creek, CA 94596, GParry@jensenhughes.com*
[3] *Curtiss-Wright Flow Control Company: 16300 Christensen Road, Suite 300, Tukwila, WA 98188, jjulius@curtisswright.com; kgunter@curtisswright.com; jgrobbelaar@curtisswright.com; mhirt@curtisswright.com*

Human reliability analysis (HRA), as it is conducted in probabilistic risk assessments (PRA), relies on the use of various models of human performance that are informed by relatively sparse data from actual experience. Such an approach can give rise to a degree of skepticism, especially when the methods produce very low probabilities of failure. At some level, there is a perception that there is a limit to the reliability of operating crews to perform a string of actions, and that available methods do not necessarily capture all the important causes of dependency. As a result, a variety of approaches have been taken to defining limiting or minimum values that should be used in lieu of low calculated probabilities. Up to this point, there has been no consensus practice in setting or using such minimum values. However, experience has shown that indiscriminate use of a lower bound joint human error probability can result in technical and process issues, such as potentially inappropriate risk ranking of resultant cutsets and very long quantification times. Furthermore, application of a floor as a means to assess unknown or unquantifiable sources dependency does not provide information on how to improve plant operational practices to enable operators to cope with accidents. This paper provides a background of dependency factors, how they are generally accounted for in PRA and Defense in Depth, and provides a proposed framework for assessing the impact of a lower bound joint human error probability in the context of risk informed decision making. This paper is derived from a more detailed EPRI report "A Process for HRA Dependency Analysis and Considerations on Use of Minimum Values for Joint Human Error Probabilities."

I. BACKGROUND

This paper is derived from a more detailed EPRI report *A Process for HRA Dependency Analysis and Considerations on Use of Minimum Values for Joint Human Error Probabilities* (Ref. 1). Human reliability analysis (HRA), as it is conducted in probabilistic risk assessments (PRA), relies on the use of various models of human performance, informed by relatively sparse data from actual experience. Such an approach can give rise to a degree of skepticism, especially when the methods produce very low probabilities of failure across a string of actions. At some level, there is a perception that there is a limit to the reliability of operating crews to perform a string of actions, and that available methods do not necessarily capture all the important causes of dependency. As a result, a variety of approaches have been taken to defining limiting or minimum values that should be used in lieu of low calculated probabilities.

Use of a lower bound joint human error probability (HEP) was initially introduced in NUREG-1792 (Ref. 2), Good Practices for Implementing HRA, as a way for analysts to ensure potentially significant accident sequences were not inappropriately truncated. The recommendation was that, "unless otherwise justified":

> 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 ~0.00001 (1E-5) since it is typically hard to defend that other dependent failure modes that are not usually treated (e.g., random events such as even a heart attack) cannot occur.

Up to this point, there has been no consensus practice in setting or using such minimum values. However, this guidance has been propagated and referenced in many subsequent guidance documents, sometimes with the lower value relaxed to 1E-6. While the original statement may not have been intended as an absolute limit, but more as a sort of trigger to have the

analyst check lower joint HEPs to see if some underlying dependence has been overlooked, it has often been interpreted as absolute.

EPRI report *A Process for HRA Dependency Analysis and Considerations on Use of Minimum Values for Joint Human Error Probabilities* (Ref. 1) provides a discussion of the issues surrounding the use of a minimum value for joint human error probabilities, documents sources of dependency that can lead to a limit on human performance, documents a systematic dependency process and provides a proposed resolution for dealing with the underlying uncertainty. Recognizing that the issue of a minimum joint human error probability is a source of irreducible uncertainty, this report was intended, not as final solution, but the beginning point for a discussion on the topic such that industry can converge on a reasonable approach at evaluating the impact of human performance in PRA.

II. ISSUES AND METHOD

There are reasons for and against implementation of a minimum limit on joint HEPs in a PRA model. The research described in Ref. 1 revealed five distinct issues surrounding the question on how and when to implement a minimum JHEP limit.

The rationale for taking a hard line approach in enforcing a specific minimum limit has been driven by three primary concerns:

Issue #1: Potentially important sequences may be truncated out of the final solution and loose visibility to the reviewer. The ASME/ANS PRA Standard requirement (HLR-QU-C1) (Ref. 3) requires analysts to identify these potentially important cutsets with multiple HFEs by quantifying the model using high values for HEPs. This process requirement alone does not alleviate this concern because, while the cutset may be identified, if the analysis is not done correctly (e.g., independence is assumed by the analyst, but not properly justified, or over-decomposition leads to unreasonably low values), then the cutset could be lost in the final quantification.

Issue #2: There is large variability in both the approach and quality of methods used across industry to address dependency, so there may be little confidence that the very low values were appropriately assessed. This is especially a problem if the cutset is lost in the final quantification.

Issue #3: Finally, there are known (e.g., safety culture, major distractions such as crew illness or injury, etc.) and unknown factors that can affect human performance that are not explicitly accounted for in current HRA methods either for the evaluation of individual HEPs or as sources of dependency. As a result, the analysis methods can produce joint HEPs with what is considered an unbelievably low value (e.g., <<1E-6). It is the collection of these factors that may constitute a fundamental limit on the performance of a crew or organization.

Application of a pre-determined minimum joint HEP across the board, if done appropriately, would ensure that all potentially important cutsets are identified and, however they are dispositioned in the final assessment, would be visible to the reviewer or regulator. These are valid concerns, and any approach at accounting for dependency must consider and address these points. However, experience with the blanket approach at applying a minimum JHEP has proven to be problematic:

Issue #4: Indiscriminate application of a minimum joint HEP proved to be, in some cases, technically inappropriate in that it can skew risk insights and risk metrics and artificially inflate the total risk metric (i.e., CDF, LERF) because of double counting that happens during the quantification process[1]. This is fundamentally contrary to the aims of a PRA, as described in NUREG/CR-2300, the PRA Procedures Guide (Ref. 4, emphasis added): PRAs should "[identify] those sequences of potential events that dominate risk and establishing which features of the plant contribute most to the frequency of such sequences," where "[k]nowledge of the most probable severe accidents

[1] This can happen because the minimum joint HEP is intended to account for a range of contexts, many of which are not scenario-specific; however, when the joint HEP is modeled, the model treats them as independent events, which leads to double counting. For example, consider two cutsets that have nominal values below a minimum joint HEP, each consists of an initiating event and three HFEs: [IE*HFE1*HFE2*HFE3] and [IE*HFE1*HFE2*HFE4]. When a minimum value of 1E-5 is applied to each of the combinations, the total risk becomes IE*2E-5. For simplicity, let us assume that the minimum value is dominated by single contributor, e.g., a crew member has a heart attack. If the joint HEP "module" were expanded into its contributors, a Boolean reduction would result in this contributor occurring only once, failing both combinations. If the probability of that single contributor is 1E-5, then the total risk should be IE*1E-5, not IE*2E-5. Because the minimum value represents an unspecified mix of scenario-specific and non-scenario specific factors, there is double counting in the quantification.

could…provide a focus for training operators to deal with [beyond design basis] accidents. Emphasis could be placed on diagnosing the most-probable severe accident sequences and on providing information and guidance to the operators on how to cope with such accidents."

Indiscriminate use of a lower bound joint HEP can result in cutsets with varying degrees of defense in depth (e.g., scenario with 2-3 recovery opportunities vs. scenarios with 4-5 opportunities) being automatically equated to each other without further thought. These risk insights and risk rankings are used to inform operations and training; if the risk insights are skewed through a systematic bias, then that could lead to poor decision making. Furthermore, application of a floor as a means to assess unknown or unquantifiable sources dependency does not provide information on how to improve plant operational practices to enable operators to cope with accidents.

Issue #5: In some cases there are significant practical challenges in attempting to apply a minimum joint HEP across the board: for some PRA models, the quantification time and effort can dramatically increase when a floor is applied, even when there is no substantial change in the risk metrics. These effects are highly plant- and model-specific.

Finally, whether or not there is a fundamental limit on human performance – and what that limit is – is ultimately an uncertainty in the PRA. When imposed quantitative limits on a joint HEP approach the risk thresholds used in decision making, then that uncertainty can become a key driver in the decision making process. In these cases, an approach needs to be taken that is consistent with risk *informed* – not risk *based* – decision making process such that the arbitrary limits alone do not dictate the decision.

The approach taken in (Ref. 1) to address these issues include:

1. Understand contributions to dependence in real operating events and cognitive failure mechanisms.
2. Review those contributions against:
    a. What is in the scope of what can be analyzed within a PRA
    b. Plant practices, defense in depth and elements of safety culture and resilience that can protect against these causes that are not accounted for in the PRA
3. Document the existing process to reduce the variability in approach across industry.
    a. Update the existing process to include insights from the literature review
4. Understand how and why the minimum joint HEP can negatively impact PRA models (technically and programmatically).
5. Provide a recommendation on the appropriate use of a minimum joint HEP, consistent with how other similar uncertainties are handled.

III. CONTRIBUTING FACTORS TO DEPENDENCY AND HOW THEY ARE ACCOUNTED FOR IN PRA

Failures in man-machine systems can happen even when the systems are designed to be highly reliable. Studies of these types of failures and their underlying cognitive mechanisms show that multiple layers of defense can be defeated by dependencies between failures of the operators to perform required actions. It can be useful to think about causes of dependence in two ways: 1) those arising from challenging unanticipated scenarios including situations that are outside the scope of procedures and training (novelty) and 2) those arising from a sufficient quantity of distractors; often, real-world disasters are a result of a combination of the two (Ref. 6).

Novelty can cause errors that propagate, for example, when, "organizations fail to perceive novelty when it is embedded or obscured by complex technology, when the complexity of the external environment outstrips the organization's ability to sense it, or when the novelty is so extreme that it cannot be accommodated in the existing worldview" (Ref. 6). Even when recognized, if the procedures and training do not offset the effect of the novelty, errors can ensue. Even when the scenario is familiar and there is guidance, such as procedures to direct the operators to the correct responses, disruptions can lead to failures of highly reliable systems when there is a sufficient quantity of distractors. For these non-novel disruptions, there can be a tipping point, where the rate of interruptions becomes greater that the rate of the organization to respond to the various distractors (Ref. 6). Cascading distractions – where the rate of new distractions exceeds the rate of response – are important contributors to severe accidents and their precursors because they overwhelm the organization's ability to respond.

Sources of novelty and non-novel distractions can come from latent conditions or emerging conditions, and often accidents are a result of a combination of the two. A review of the literature (Ref. 5-15) produces a list of contributors to dependent failures, many which have been observed in real-life scenarios. While this is not intended to be an all-inclusive

list, the list below provides at starting point that we can use to understand 1) how causes of dependency arise and are mitigated by plant practices and 2) to what extent these factors are, and can be, analyzed in a PRA. These causes can lead to novelty (e.g., mismatch between reality and expectations) or can contribute to cascading distractions that can overwhelm the organization's ability to respond; in this way, the list is a mix of causes and contributors. It should be noted that most real events include a combination of many of these factors discussed below.

- **Common cognitive failures for multiple responses**
    - *Common erroneous mental model of the plant status that affects alternative recovery actions for same safety function* (e.g., an incorrect mental model formed of the plant status could lead the crew to dismiss or discount data that would indicate correct response).
        - Incorrect mental models could be caused by differences between the actual and practiced scenarios (mismatch between expectation and reality) in the timing or other aspects of the event progression. These differences can arise from latent conditions:
            - Differences between simulator and reality
            - Inadequate technical knowledge regarding underlying condition (e.g., frazil ice at Wolf Creek (Ref. 15))
            - Errors in procedures, ambiguous procedure or mismatch of procedures to scenario (usually from subtlety of design or partial failures)
            - Unknown design errors or failure of non-modeled systems (e.g., I&C)
            - Failure to tag out known issues
            - Frequent training on subtly different scenario
    - *Common erroneous mental model that persists throughout the accident scenario*
        - For an erroneous mental model to persist throughout the complete accident scenario, the initially formed mental model would have to be sufficiently strongly held that it would interfere with the correct recognition of subsequent responses. Given the extent to which EOPs are tested and validated, such an incorrect mental model would almost certainly have to be caused by a significant latent condition, such as:
            - Mismatch between the simulator plant response model and the specific scenario
            - Significant unidentified errors in procedures that would lead operators into an incorrect response path
            - Significant indication errors
        - In the past, "confusion matrices" have been used to identify accident scenarios that have similar signatures that can cause confusion. Symptom-based procedures have mitigated this issue to some extent.
    - *Failure to recognize and understand a common cue indicates the need for multiple responses.*
        - This may be due to factors such as human-machine interface problems, training deficiencies or unfamiliarity of the scenario.
- **Common contextual impact of performance influencing factors (PIFs)**
    - For example, persistence of high workload, cascading distractions, time pressure, environmental stress, etc. throughout the scenario can impact the entire response.
    - These conditions may occur when having to perform responses close in time for example or can arise from a host of miscellaneous distractors from extraneous sources that can persist over the course of the accident, including:
        - Injury or Illness, such as: Physical illness (e.g., heart attack, stroke, seizure) or Mental illness (e.g., workplace violence).
        - Poor crew dynamics
        - Partial or extraneous failures (e.g., non-PRA failures) that divert attention from the more important failures or indications.

  - This could be due to an inadequate corrective actions program which fails to correct known problems or can be unanticipated random failures (e.g., in one event (Ref. 9) a field operator bumped a breaker, tripping it and causing accidental loss of power to an instrument bus, complicating the scenario).
  - Latent failures can be a significant contributor to this category; real events have shown a ratio of 4:1 of latent to active failures in real events (Ref. 13).

- **More challenging context as a result of the consequences of prior error**
  - This can manifest itself as decreased time for response, increased stress, deteriorating or difficult plant conditions, etc.
  - This is a form of functional dependence that is a natural consequence of the sequence. Errors of commission may be a cause of this type of dependence, but are typically not modeled unless a compelling context is identified (e.g., spurious operation of I&C during a fire).
  - The accumulation of small individual failures may also be an important factor here. Ref. 15 provides a summary of experience extracted from 35 operational events and found that most of these events exhibited between 6-12 small individual failures which were not individually significant, but had a cumulative effect.
- **Organizational factors and safety culture deficiencies**
  - These types of issues typically underlie some of the causes and contributors described above. This can be a large contributor to latent failures, which is a major component of real accidents.
  - Causes of failure and dependence can result from factors such as:
    - Incompatible work activities
    - Inadequate maintenance practices or testing after equipment service
    - Failure to enforce standards
    - Lack of trust in procedures or inadequate procedures
    - Failure to correct known problems
    - Safety culture issues such as compressed outage schedule (e.g., may have extra manpower, but resources are diverted to efforts to get the outage back on schedule instead of addressing the problem at hand)
    - Failure of questioning attitude
    - Poor communication or command and control/situational awareness (e.g., due to non-standard crew composition, poor crew dynamics, etc.)
  - "The most commonly-occurring failures observed in [the review of 35 NPP operating events] stemmed from command and control deficiencies; inadequate maintenance practices, inadequate procedures, failure to correct known deficiencies, failure to respond to industry notices, failure to enforce standards, and inadequate testing after equipment service." (Ref. 15)

Only some subset of these factors are, and can practically be, modeled in a PRA. A PRA model is a representation of the spectrum of potential accident scenarios. The accident scenarios constructed for a PRA are idealized, representative scenarios each of which typically represents the bounding case for the whole class of scenarios with similar characteristics. Where the scenarios that are encompassed by the representative accident scenario differ is in a level of detail that is not modeled. Examples of assumptions that are inherent in the definitions of the representative accident sequences include:

- Partial failures are not modeled. Failures of components are considered as complete, e.g., a valve fails to close and remains in the open position as opposed to in a half-closed position.
- Failures occur at the time the supported function is demanded, i.e., failures to run are assumed to occur at the time of demand and not when the failure actually occurs. This essentially limits the time at which subsequent responses are called for.
- Failures that have no direct impact on the accident scenario development are not modeled (e.g., coincidental failures that do not impact the accident progression, but may cause distraction).

While they may not be stated explicitly, unless otherwise specified, the following assumptions are implicitly made for the identification and functional definition of the human failure events (HFEs) to be included in the PRA model:

- Operators trust and follow their procedures. Therefore, accident sequences are developed based on the expected procedure progression given the initiating event. Without this assumption, bounding scenarios cannot be developed. One consequence of this is that errors of commission or deliberate violations of procedures are not typically modeled.
- The set of operating procedures (EOPs, AOPs, annunciator response procedures, system operating procedures, etc.) that guide the responses whose failures are represented by the HFEs have been tested and verified to be appropriate.
- Training is conducted on the procedures such that the methods of response are understood and have been practiced in the simulator or, for some of the more unexpected responses, using desk-top exercises.
- There is sufficient fidelity between the plant response to a given set of failures or an initiating event as modeled in the simulator and the expected plant response that there will not be any significant potential for developing an inappropriate understanding of the plant status and the required operator responses.
- The crew is experienced, well trained, and well-disciplined with good communication protocols. The crew complement (shift staffing) is in accordance with the licensing requirements.
- Instrumentation required to implement the operating procedures is available and reliable. When instrumentation is significantly impaired, this will be explicitly modeled and reflected in the value of the HEP. However, depending on the nature of the indications, single instrument failures are often considered to be compensated for by redundant instruments.
- Finally, not all things that could affect the reliability of the operators' response can be modeled. However, it is assumed that the procedures and training of the operators are flexible enough for the scenarios for which they have been designed that they enable coincidental but unimportant distractions to be dealt with appropriately.

The functional definition of the HFEs identifies those performance influencing factors (PIFs) that are scenario specific. Depending on the HRA method used, additional performance influencing factors are taken into account when evaluating the HEP. These PIFs characterize the scenario-specific context that influences the reliability of the operators' response.

An important assumption of all HRA models is that, because the time at which an initiating event may occur is considered random, the HEPs are intended to represent an average over crews, time of day, and other plant conditions that could be coincidental and are not such that attention is essential, but could potentially be distracting. With respect to the last point, the assumption is that following the EOPs and AOPs has priority over non-essential, non-safety-related conditions. Thus the PIFs that are taken into account are those that are systematic and not those that affect individual crews.

In principle, if the set of PIFs used to evaluate individual HFEs were all inclusive, this should be sufficient to address the dependence between the successive HFEs. However, each HRA method only looks at a simplified sub-set of PIFs and general do not examine more subtle contextual factors such as: incompatible work activities, failure to tag out failed or unavailable equipment (transient conditions), design errors or failures in non-modeled sub-systems, partial failures, crew injury or illness, etc. While these are all potential causes that could influence the crew's ability to perform the correct response – or cut across multiple responses - there is no way to effectively quantify them.

Effectively, there are classes of performance influencing factors that are considered to be outside the boundary of the assumptions typical in an HRA and therefore, not explicitly captured in the HEPs. Of particular interest for the purposes of discussing a bound on the joint HEP are those that have the potential to create a context where the likelihood(s) of the HFE(s) following the first chronologically occurring HFE are increased over and above any dependence already accounted for.

Current dependency methods, such as the EPRI dependency analysis method described in Section 3 of (Ref. 1), typically use a combination of modeling techniques and assessment of linking factors to account for dependency. Modeling techniques include explicitly capturing cognitive dependencies by modeling common cognitive events in the fault tree or event tree logic; common cognitive events capture dependencies that arise from the fact that two responses may share a common cue or procedural step. The EPRI dependency analysis method also evaluates a set of linking or dependency factors that account for some of the dependency factors listed above by proxy.

A special note must be made here regarding other PRA modeling assumptions commonly made. The intent of the PRA is to provide an accurate risk picture and relative risk ranking by using a model that reflects our best state of knowledge. One of the necessary balances in a PRA is between level of detail and level of knowledge – adding additional complexity to a model does not inherently improve the accuracy of that model. As such, the assumptions made in the HRA assessment should be consistent – to the extent possible – with the assumptions made in modeling other parts of the PRA (e.g., initiating events, equipment failures, etc.). Some of these assumptions include: absence of design and construction failures, stable parameters (no wear-in/wear-out phase), elimination of failure events from equipment reliability data whose causes have been eliminated through administrative or other measures, modeling of common cause failures, exclusion of intersystem common cause failures, etc. The same organizational and cultural deficiencies that can cross multiple defense barriers in a human response can also cross multiple barriers in the equipment response or the combination of human and equipment

response. These are not generally dealt with explicitly in PRA, but rather it is assumed that they would be dealt with through performance monitoring of the organization and through additional defense in depth measures.

Finally, many of these contributors that are not explicitly accounted for in the HRA – such as organizational factors and safety culture – are actually overarching issues, not scenario-specific, and their scenario-specific manifestations cannot be known a priori. Thus, accounting for these factors in the quantification by systematically increasing the joint HEPs provides little value to decision-making. However, it can be useful to know that some scenarios may be more able to tolerate these deficiencies. Elements that increase the resilience of an operator response include:

- Long time frames with limited interruption and sufficient resources
- Independent perspectives (TSC, ERF, shift change, STA, etc.)
- Symptom based procedures
- Strong and recurring cues with time for recovery
- Independent cues
- Lack of competing priorities
- Similarity of response to training

The recommended approach described below will discuss how these factors can be considered qualitatively to provide confidence to a decision maker that an accident scenario has sufficiently high reliability that it can be considered negligible due to scenario-specific causes.

IV. HOW TO ADDRESS UNCERTAINTY AROUND THE MINIMUM JOINT HEP

Fundamentally, the issue driving the application of a minimum joint HEP is one of uncertainty. Therefore, the process used to address this source of uncertainty should be consistent with the general framework for addressing uncertainties in risk-informed decision-making. Derived from principles and process outlined in NUREG-1855, Rev. 1 (Ref. 16) and EPRI 1026511 (Ref. 17), and tailored for this specific application, Figure 1 describes a recommended process for evaluating the impact of a minimum joint HEP in risk-informed decision-making.

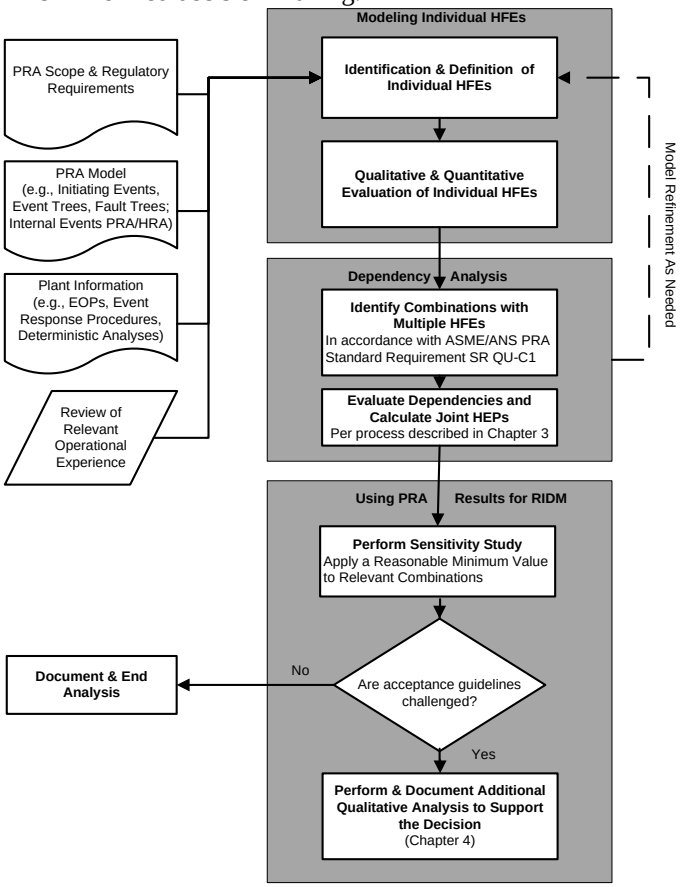

Fig. 1: Process for Evaluating HFEs and Using the Results in Risk-Informed Decision-Making

It is important to note at this stage that, while the guidance here is specific to HRA dependency – particularly where there are very low joint HEPs – the process is generic to assessing all key uncertainties arising from the HRA. The issue being assessed here is whether there are potential mechanisms that would lead to a higher joint error probability of the operating crew successfully responding to plant accidents than the HRA methods with dependency rules applied would predict. Therefore, the approach proposed for addressing this issue can be described as consisting of four steps, as follows:

1. Evaluate the Decision Using the Base PRA model. The base PRA model, sometimes referred to as the "model of record", is intended to represent the "best estimate" representation of the as-built, as-operated plant, and includes a "best estimate" HRA. A structured dependency analysis with a reasonable technical basis, such as the dependency process discussed in Section 3, should be performed and included in the PRA. No minimum joint HEP should be included at this stage (unless it is used as a screening-type value to replace a detailed dependency analysis[2]). This is the best-estimate PRA analysis.

2. Perform a Sensitivity Study: A sensitivity study should be performed using a specified minimum joint HEP to understand if the acceptance guidelines are challenged as a result of the uncertainty.

   The application of the base PRA will have identified those HFE combinations that are significant to the risk metrics using the dependency rules of the HRA methodology being applied, and their dependence will have been addressed in the context of the accident sequences in which they occur. The purpose of the sensitivity analysis is to identify those additional HFE combinations that would become important to the decision when a minimum joint HEP is applied.

   In this step, a reasonable minimum value should be used as a sensitivity study. What constitutes a "reasonable" minimum value depends on what is being modeled. For example, for internal events, a reasonable value might be 1E-5 or 1E-6. Although neither of these values has a particular technical basis, they have both been historically used in this context and are convenient in that they coincide with commonly used decision thresholds. For external events (e.g., seismic), a graded minimum value might be appropriate, applying a higher minimum HEP for very high hazard values. For extremely long time windows such as may be found in a shutdown PRA, going below 1E-6 is difficult to justify empirically, so this step should be conducted using a 1E-6 joint minimum HEP.

   Note, the minimum joint HEP sensitivity study should be performed by applying the minimum joint HEP to all identified combinations. There is the potential for HFE combinations which were previously truncated from the solution to appear in the sensitivity results because the HFE combination with the minimum joint HEP applied may now rise above truncation.

   At this stage, the results of the sensitivity study should be evaluated against the acceptance criteria for the decision. If the acceptance criteria are not challenged (e.g., Figure 2), then it is sufficient for the analyst to document the sensitivity analysis and end the analysis. If, however, the sensitivity analysis challenges the acceptance guidelines, then the minimum joint HEP is a key source of uncertainty and needs to be further examined in Steps 3 and 4.

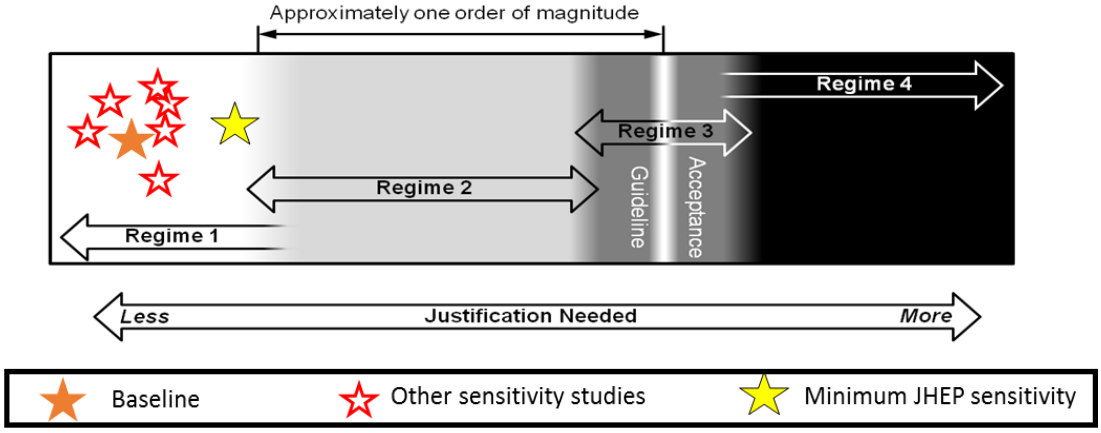

Fig. 2: Assessing the Impact of the Sensitivity Study Against the Acceptance Guidelines

[2] This is the type of approach described in EPRI 1021081 (Ref. 5)

3. Identify Related Accident Scenarios: If the acceptance guidelines are challenged, then the minimum joint HEP becomes a key source of uncertainty. The analyst must then evaluate the model to identify the important contributors to the risk increase, which need to be examined in more detail in Step 4.

   The point in this step is to understand why this is a key source of uncertainty, and what are the accident scenarios that contribute substantially to the risk increase. For the purposes of this document the term "accident scenarios" is meant to include any or all of the following: a single cutset, a group of cutsets, an event tree sequence, and/or a group of event tree sequences. This step is accomplished by reviewing the results of Step 2 using the following process.

   First, for the joint minimum HEP that impacted the acceptance criteria in Step 2, review the events represented by the terms other than the joint minimum HEP to confirm the modeling (i.e., confirm that it is a valid scenario). This typically consists of the initiating event(s) ANDed with other events such as random failures in automatically actuated systems, and may include spatial impacts such as fire, flood, or seismic (if applicable). This may not be straightforward since the spatial impacts may or may not be represented by explicit events in the PRA model. The review should confirm that the modeled PRA context (defined as the initiating event followed by successes and failures of SSCs) has led to a demand for operator action(s) in order to prevent core damage or release.

   Second, identify what initiating event and what functions are contributing to the need for operator action. This is typically started during the base case dependency HRA evaluation, as the analyst identifies combinations of HFEs that tend to repeat. These may be following a specific initiating event or a group of initiating events. For example, in the decay heat removal function, the failures of the different methods available for decay heat removal are ANDed together; the same combination of methods are demanded after each initiating event, unless some methods are precluded by the impact of the initiating conditions (e.g., a fire). On the other hand, restoration of a source of electrical power is typically only included in the Loss of Offsite Power and Station Blackout event trees, and actions to compensate for failure of control rod insertion typically only apply to ATWS event trees.

   The output of this step should be the identification of those PRA accident scenarios where the joint minimum HEP is impacting the acceptance criteria of the decision, culled from Step 2, plus the identification of the PRA context consisting of applicable initiating events and SSC success and failures that have led to the demand for operator actions. This information will be used in the development of the operational narrative in Step 4.

4. Construct Operational Narrative: For the important contributors identified in Step 3, operational narratives should be constructed in sufficient detail to provide the decision maker with the qualitative understanding of why the base case is or is not justified. The operational narrative should not only describe those scenarios where the joint minimum HEP is potentially important, but also describe how the plant procedures and operational practices are effective in preventing postulated causes of dependence from interfering with the operating crew's ability to successfully mitigate the accident sequence. Here the PRA results will be weighed against the other elements of risk-informed decision-making to determine if the application is acceptable or if modifications need to be made to the application and/or plant operations.

   This step has four elements; each of which are described in more detail, with an illustrative example, in (Ref. 1):

   - Construct operational narrative and timeline (confirm baseline analysis)
   - Consider other elements of risk-informed decision-making (e.g., defense in depth, safety margins and performance monitoring)
   - Provide feedback to operations (as needed)
   - Provide an assessment for the decision-makers to support the decision

   Commensurate with the importance of the application and nearness of the sensitivity result to the acceptance guidelines, by the end of this step, the analyst will have a strong understanding of the impact of the uncertainty and the qualitative strength of the operational narrative and defense in depth features to weigh against that uncertainty. At this point the analysts can either accept the uncertainty, document and end the analysis; or propose a compensatory action if they feel that the uncertainty is too high. In either case, the process will likely yield feedback for operations that can improve performance.

V. CONCLUSIONS

Highly reliably organizations can fail, and these failures are often due to a string of human errors or organizational deficiencies at different levels. These failures can be active or latent, and often significant events include a mix of the two.

Through a review of the psychological literature and operational events, we can understand some of the factors that can affect human performance. Some of these factors, however, cannot be explicitly accounted for in current HRA methods either for the evaluation of individual HEPs or as sources of dependence. Furthermore, there may be unknown factors that can affect dependence. It is the collection of these known and unknown factors that are thought to constitute a fundamental limit on the reliability of a crew or organization.

Not all of these factors can – or should – be explicitly accounted for in a PRA model. PRA models have a certain scope and set of underlying assumptions. For items that fall outside that scope and assumption set, other principles of risk-informed decision-making are used to provide supplemental information that can build additional confidence in the analysis. Some of these dependency factors – including organizational and safety culture issues – are not necessarily scenario specific, and mature methods do not exist to analyze their impacts. Therefore, those factors that cannot be reasonably assessed and do not change the risk rankings directly, are excluded from the scope of the PRA. Instead, elements of defense in depth, performance monitoring and operational resilience are expected to mitigate such failures across the board. Some of these elements include quality assurance programs for procedures and human-machine interfaces, reactor oversight on human performance, etc.

Furthermore, indiscriminate application of a minimum joint HEP to account for these factors can be problematic. In some cases, application of a minimum value can be technically inappropriate in that it has the potential to skew risk insights and risk metrics and artificially inflate the total risk metric (i.e., CDF, LERF) because of double (or multiple) counting of a single cause during the quantification process. This in turn can lead to incorrect or masked insights and poor decision-making. In other cases, it can cause a dramatic increase in the quantification time and effort, even when there is no substantial change in the risk metrics. Fundamentally, however, requiring a minimum value does not allow screening or truncation of scenarios that the plant is designed and equipped to handle with high reliability.

This does not mean that the question of limits to human performance should be overlooked. To appropriately account for dependencies in human response within a PRA model, the following items need to be implemented:

1. All relevant HFE combinations must be identified to prevent improper truncation during final quantification. This can be accomplished by solving the model using HFEs set to a high value (e.g., 1.0) for identification.

2. Dependencies amongst HFEs within an accident sequence cutset must be assessed using a consistent and systematic approach. While this approach may not necessarily account for all possible sources of uncertainty – which is not possible given the current state of knowledge – it should capture the major factors that can increase the probability of failure and differentiate between scenarios.

3. Finally, there should be some consideration of uncertainty of the analysis on the final results. One method is to use a minimum joint HEP value as a sensitivity study as a way to address uncertainty in the context of a specific decision. If the sensitivity study reveals a combination(s) that dominates the risk or challenges acceptance guidelines, this combination(s) needs to be analyzed qualitatively to determine whether or not the combination(s) can be treated as negligible. In this approach, the base model would retain the joint HEPs calculated by the original dependency analysis unless otherwise indicated by the results of the qualitative analysis.

The approach provided in this document is only one potential solution to the issue of how to deal with limits to human performance within a PRA. The impact of indiscriminate application of a minimum joint HEP is highly plant and model specific. There are many variables, ranging from plant design to modeling choices, which determine the impact a minimum joint HEP can have on the quantification process and results. Other solutions that have been applied include:

- Keeping a minimum joint HEP in the base model (when it does not substantially impact quantification)
- Using the minimum joint HEP in the base model with relaxation only for selected scenarios. In this case, using qualitative arguments to lower the minimum value used in the base model (e.g., to 1E-6, 1E-7 or 0) for combinations that are qualitatively assessed to be negligible, but dominate the results when a specific minimum joint HEP is applied. Note, for this approach, the guidance provided in Section 4.2 and Appendix A can be used to determine which scenarios can be relaxed.
- Applying a graded minimum joint HEP in lieu of a detailed dependency analysis

These, and other, approaches, while different from what is recommended here, may also be reasonable solutions. The larger point to keep in mind is that quantitative uncertainties should not be the primary driver for decisions; sensitivity studies and a good qualitative analysis, coupled with considerations of other elements of risk-informed decision-making, can lend confidence to the results of the PRA model.

ACKNOWLEDGMENTS

EPRI would like to acknowledge the contributions of members of the Dependency Committee of the EPRI HRA Users Group for providing data, examples and feedback on the recommended approach described in EPRI 3002003150, from which this paper is derived. The authors are especially grateful for the support of Mark Averett from NextEra Energy, Inc. As chairman of the HRA Users Group and a reviewer of early drafts of the document, he provided a valuable user perspective for the direction of this report.

REFERENCES

1. *A Process for HRA Dependency Analysis and Considerations on the Use of Minimum Joint HEP Values*, EPRI-3002003150, Electric Power Research Institute, 2016.
2. NUREG-1792, *Good Practices for Implementing Reliability Analysis*, U.S. Nuclear Regulatory Commission. A. Kolaczkowski, J. Forester, E. Lois and S. Cooper, April 2005.
3. ASME/ANS RA-Sb-2013, *Addenda to ASME/ANS RA-S-2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications*, The American Society of Mechanical Engineers, New York, NY, February 2013.
4. NUREG/CR-2300, *PRA Procedures Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants*, U.S. Nuclear Regulatory Commission. J.W. Hickman, A. Gilbertson, G. Parry, J. Lehner, G. Martinez-Guirdi, J. La Chance and T. Wheeler, March 2013.
5. *Establishing Minimal Acceptable Values for Probabilities of Human Failure Events*. EPRI, Palo Alto, CA: 2010. 1021081
6. J.W. Rudolph, N.P. Repenning. "Understanding the Role of Quantity in Organizational Collapse," from Administrative Science Quarterly vol. 47, no. 1. March 2002. Pgs. 1-30.
7. NUREG-2114 NL/EXT-11-23898. *Building a Psychological Foundation for Human Reliability Analysis*, U.S. Nuclear Regulatory Commission. E. Lois, et. al., August 2012.
8. NUREG-2199, Vol. 1, Rev. 0, *An Integrated Human Event Analysis System (IDHEAS) for NPP Internal At-Power Application*, U.S. Nuclear Regulatory Commission. J. Xing, G. Parry, M. Presley, J. Forester, S. Hendrickson, and V. Dang, V. In Press (2016).
9. US NRC Licensee Event Report LER 261/10-002. *Final Precursor Analysis of H.B. Robinson Electrical Fault Causes Fire and Subsequent Reactor Trip with a Loss of RCP Seal Injection and Cooling*. September 23, 2011. ML112411359.
10. NUREG-1880. *ATHEANA User's Guide*. U.S. NRC, Washington DC: 2007.
11. NUREG-1624. Revision 1. *Technical Basis and Implementation Guidelines for a Technique for Human Event Analysis (ATHEANA)*. U.S. NRC, Washington DC: 2000.
12. NUREG/CR-6265. *Multidisciplinary Framework for Analyzing Errors of Commission and Dependencies in Human Reliability Analysis*. Brookhaven National Laboratory, Upton, NY. M. T. Barriere, W. J. Luckas, J. Wreathall, S. E. Cooper, D. C. Bley, and A. M. Ramey Smith August 1995.
13. J.N. Sorensen, "Safety Culture: a survey of the state-of-the-art", *Reliability Engineering and System Safety* vol 76. 2002. Pg. 189-204.
14. U.S. NRC Memorandum from Jack E. Rosenthal (Chief of Regulatory Effectiveness and Human Factors Branch of the Office of Nuclear Regulatory Research) to John T. Larkins (Executive Director of the Advisory Committee on Reactor Safeguards), Subject: *Meeting with the Advisory Committee on Reactor Safeguards Human Factors Subcommittee, March 15, 2000, on SECY-00-0053, "NRC Program on Human Performance in Nuclear Power Plant Safety."* March 6, 2000. ML003689518. Attachments to Memo:

i) "Summary of INEEL Findings on Human Performance During Operating Events." Report No. CCN 00-005421, Transmitted by letter, February 29, 2000. (Attachment 1)

ii) "Accident Sequence Precursor (ASP) Qualitative Analyses." (NRC Staff) (Attachment 2)

iii) O'Hara, John M., and Higgins, James C., "Risk Importance of Human Performance to Plant Safety," Brookhaven National Laboratory, Report W6546-T1-2-10/99, Transmitted by letter, February 28, 2000. (Attachment 3)

iv) "Human Performance Programs at Other Agencies." (NRC Staff) (Attachment 4)

15. NUREG/CR-1278, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications* (THERP), U.S. Nuclear Regulatory Commission. A. D. Swain and H. E. Guttman, August 1983.

16. NUREG-1855, Rev. 1, *Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision-making*, U.S. Nuclear Regulatory Commission. M. Drouin, et al. In Press (2016).

17. *Practical Guidance on the Use of Probabilistic Risk Assessment in Risk-Informed Applications with a Focus on the Treatment of Uncertainty.* EPRI, Palo Alto, CA: 2012. 1026511