A working draft, in-progress report

The General Methodology of an Integrated Human Event Analysis System (IDHEAS)

Draft Report: 3/4/2016

Prepared by:
Jing Xing, Y. James Chang

U.S. Nuclear Regulatory Commission

1 INTRODUCTION AND OVERVIEW

1.1 Introduction

1.1.1 Background

Probabilistic risk assessment (PRA) results and insights have been used to support risk-informed regulatory decision making by the U. S. Nuclear Regulatory Commission (NRC). Human reliability analysis (HRA) is an essential part of PRA. HRA is an engineering approach to systematically analyze human performance for known and unknown situations. Performing HRA requires both qualitative analysis (i.e., analyzing the human event) and quantification (i.e., estimating human error probabilities, HEPs). The insights an HRA can provide include 1) development of an operational narrative describing imperfect, unexpected, and non-typical conditions that challenge human performance, 2) Identification of human actions that may lead to undesired or unsafe plant status, 3) potential ways that crews may fail to perform required actions, 4) situational factors that impact crew performance, and 5) estimation of the likelihood of personnel failing to perform the actions. Over the last 40 years, HRA has been shown to provide a meaningful tool supporting safety regulation.

To date, there have been about fifty HRA methods developed domestically and internationally. In the U.S., notable HRA methods used in the nuclear industry include THERP, ASEP, SLIM-MAUD, SPAR-H, ATHEANA, FLIM-MAUD, HCR/ORE, and CBDT. Improving HRA has been a focus of the NRC since the publication of NRC's PRA policy statement [1] and the NRC has published guidance on practicing HRA with the various HRA methods [ref**]. Yet, there are several areas in HRA that can be improved:

Application scope – Each existing HRA method was developed for a specific application domain, and most of them were developed for internal events in nuclear power plants (NPPs); as the result, the methods are not adequate to model human actions in external NPP events and non-NPP domains. PRA is being applied in a growing number of different domains of application (e.g., at-power, shutdown, inside the control room, outside the control room, procedure driven actions, actions taken based on "knowledge," in the sense that crews would need to understand from their general plant knowledge what procedure to use). Recently the NRC has approved performing a Level III PRA with the objective of analyzing the risk contributions from all potential sources, internal and external events associated with the reactor as well as events associated with other sources, such as the spent fuel pool. As the application of PRA grows and covers more contexts, HRA must be able to expand with it and support the growth areas. Over the years, some HRA studies have been performed for contexts other than internal at-power events. The studies either adapted the methods used for internal at-power events or employed the general HRA concepts and process without using any specific methods. A consistent methodology is needed.

HRA variability – HRA results, especially the human error probability (HEP) for a particular human failure event (HFE) can vary depending on the HRA model/method used and/or the

analyst applying the method. The international HRA benchmarking study demonstrated that key sources of variability included weak guidance on qualitative analysis and poor understanding of performance influencing factors (PIFs) that affect HEP estimates [4-5].

Scientific basis – The use of research findings and theory related to human cognition in existing HRA methods was generally limited; most HRA methods were built on behavioral observation of human performance without modeling the intrinsic mechanisms of human cognition underlying human errors. This could lead to different interpretations of the same observed phenomena in practicing HRA and poor understanding of the causes of human performance errors.

Data for HRA – The use of empirical data for HEP estimation in existing HRA methods was limited due to the lack of relevant data and discrepancies between the formats of available data and HRA methods. Lack of a strong data basis in the methods may challenge method validity and introduce variabilities in HEP estimation.

The HRA discipline's perception of system risk associated with human error has significantly changed in the past two decades. This change has caused the development of an array of so-called "second-generation" HRA methods. The second-generation HRA methods are distinguished from first-generation methods by their emphasis on human cognitive processes. Second-generation methods identify the contexts that would likely cause failures in human cognitive processes when performing a task of interest, resulting in human failures in the PRA scenario. This approach sees that human error could occur not only randomly but also systematically. The human cognitive models behind the second-generation methods are used to explain how a human error would occur and explain the associated error types and error causes. The human-centered approach of second-generation HRA methods provides a convenient framework with a sound theoretical foundation to address various hazards (e.g., hardware failures, fire, flood, earthquake, and high wind, etc.) occurring during different operational modes (e.g., at-power and shutdown) from various radioactive sources (i.e., reactor, spent fuel handling, and dry cask storage) across PRA level 1, 2, and 3 event severity. The required considerations to assess the human contribution to the risk of these operations, in an adequate and practical manner, exceed the scope of most HRA methods mentioned above.

1.1.2 HRA method development – An Integrated Human Event Analysis System (IDHEAS)

In a Staff Requirements Memorandum (SRM) (SRM-M061020) [2] to the Advisory Committee on Reactor Safeguards (ACRS), the Commission directed staff to "evaluate the different human reliability methods in an effort to propose a single model for the agency to use or guidance on which model(s) should be used in specific circumstances." The Office of Nuclear Regulatory Research (RES) took the lead to address SRM-M061020. The RES staff decided to develop an enhanced HRA method, referred to as the Integrated Human Event Analysis System (IDHEAS), which addresses the areas for improvement listed in Section 1.1.1 above. The general methodology described in this document integrates the strengths of existing HRA methods with

new developments based on IDHEAS to improve HRA. The IDHEAS approach is intended to improve HRA with the following features:

A general methodology – IDHEAS provides a general HRA methodology consisting of a process for performing qualitative analysis and a Basic Quantification Structure (BQS) from which application-specific quantification models can be developed; The BQS includes a generic set of cognition-based crew failure modes, cognitive mechanisms underlying the failures, and a comprehensive list of PIFs. Thus, the general methodology is application-independent and can be used for HRA in different domains. The fact that various application-specific HRA models all originate from the IDHEAS general methodology is expected to reduce method-to-method variability.

Enhanced scientific basis – IDHEAS is based on state-of-the-art of cognitive science and it models human cognitive activities in a teamwork and organizational environment. Human cognitive activities are described through the five basic macrocognitive functions: detecting information, understanding the situation, making decisions and response planning, executing actions, and teamwork. Cognitive mechanisms of human performance are built into the methodology and serve as a foundation to analyze human performance errors.

Enhanced guidance to reduce HRA variability – IDHEAS delineates a structured HRA process for consistently analyzing an event and transparently documenting the results; IDHEAS also provides step-by-step guidance for qualitative analysis and quantification that clearly specifies the objective, process, inputs and outputs of each step. This detailed guidance is expected to reduce analyst-to-analyst variability.

A built-in interface with HRA data – The IDHEAS General Methodology supports the analysis and documentation of the cognitive elements of human behaviors in an event. The structure makes it possible to use human error data from other events or domains that share cognitive aspects with the event being analyzed. A related staff effort is the development an HRA database to address SRM ** on using empirical data for HRA. The database, referred to as SACADA [ref**], is structured on the same cognitive framework as that in IDHEAS to directly support HEP estimation.

1.1.3 Strategic Approach to HRA Method Development

The project started from an understanding of the strengths and weaknesses of existing HRA methods. The project team performed a review of existing HRA methods and also synthesized the lessons learned from the HRA International Benchmarking study [NUREG/IA-0216]and the US Empirical Study [NUREG-2156] where different HRA methods were used to analyze a common set of human failure events. The main conclusions of the team's review are summarized in the following:

1) Most methods were developed with prospective operator actions in response to internal, level 1, at-power events. The operators' actions in this context are directed by abnormal

response procedures or emergency response procedures. These procedures typically are well written and constantly revised based on routine operator training. The US plants require that their operators adhere to procedure instructions.

2) Each existing method evaluated has its own strengths and application scope. A single, existing method cannot adequately address all of the NRC's HRA needs. Recommending a pool of HRA methods for use without substantial revision to the HRA methods would not effectively address the issues of method-to-method variability and analyst-to-analyst variability.

3) The existing methods do not have an explicit cognitive basis for why and how humans fail to perform tasks. Every second-generation HRA method that implicitly or explicitly has a human cognitive/behavior model as the modeling foundation fails to explicitly describe, with sufficient detail and coverage, the connection between the cognitive/behavior model and the implementation of the HRA method. To a certain degree, the quality of HRA results is strongly dependent on the analysts.

4) The methods either lack guidance for qualitative analysis or lack the interface between qualitative analysis and quantification of HEPs. A good qualitative analysis is the foundation for a good quantitative analysis (i.e., assessing HEPs). Most HRA methods refer to using the SHARP1 process for conducting qualitative analysis. Some HRA methods (e.g., THERP and ATHEANA) provide guidance on conducting qualitative analysis. However, these methods do not provide explicit instruction on how the information obtained from the qualitative analysis is used in estimating the HEP values.

5) The methods are ambiguous regarding guidance for assessing the statuses of the factors specified in the methods to estimate HEPs. The factors are generally referred as performance influencing factors (PIFs) or performance shaping factors (PSFs). This document uses PIFs to represent the factors that affect HEPs. At a high level, most second-generation HRA methods provide sufficient coverage of the effects on human performance. However, the connection between the methods identified PIF and the foundational human cognitive/behavior model implicit in the methods is not adequately explained. This gap affects the quality of the use of the PIFs for estimating HEPs.

Based on the team's review and analysis, the staff decided to take the following approach in addressing the SRM-M061020:

1) Develop a cognitive basis for HRA that addresses the following questions: How do humans perform complex cognitive tasks? What makes humans reliably perform tasks? What causes human failures (failing to reliably perform tasks)? The cognitive basis describes the fundamentals of human cognition and is applicable to human performance in any context. The results are documented in NUREG-2114 "Cognitive Basis for HRA."

2) Develop a generic HRA methodology and document its concepts and process, and provide implementation guidance. This methodology should be based on the cognitive mechanisms underlying human errors, integrate the strengths of existing HRA methods

and good practices, and conform to existing PRA/HRA standards and guidance. We refer to this methodology as *an Integrated Human Event Analysis System - General Methodology (IDHEAS-G).*

3) Implement the methodology in the context of internal, at-power, level 1 events. Because human tasks in this context are well defined in operating procedures, we are able to develop specific crew failure modes and decision trees representing the effects of contextual factors on the failure modes. HRA analysts can use this implementation in analyzing internal, at-power events and may adapt it to other contexts where human actions are well defined through procedures. The work is a collaboration with EPRI and is documented in NUREG-**** [Ref**] "*IDHEAS Internal at-Power Application."*

4) Develop application-specific quantification models for other applications or domains from the Basic Quantification Structure in IDHEAS-G.

Figure 1-1 illustrates the above strategic approach. As discussed above, documentation of the cognitive basis and application of the method to internal, at-power, level 1 events have been published in previous NUREGs. This document describes the IDHEAS - General Methodology for application to the broader context of NPP safety.

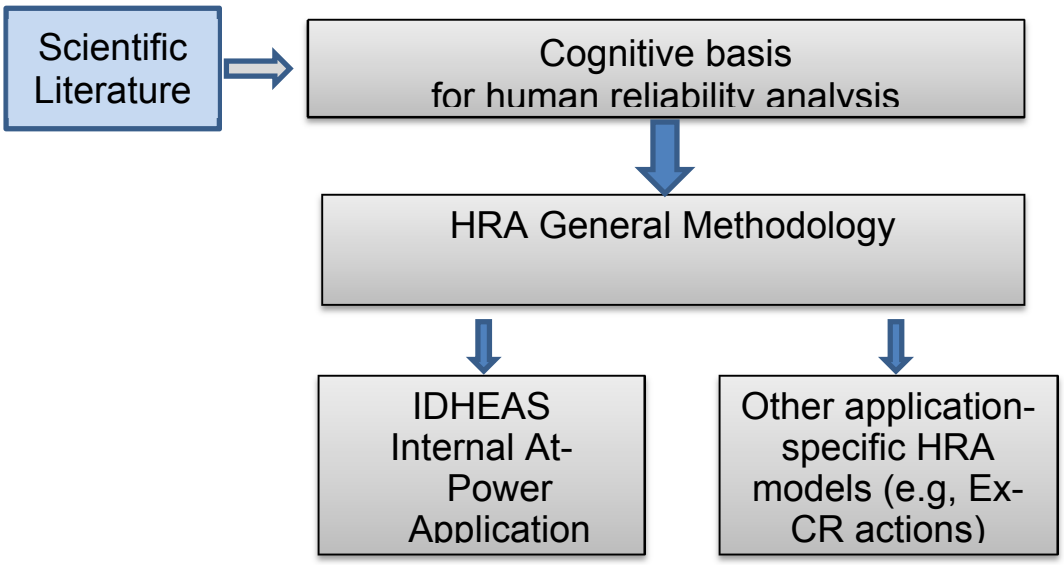


Figure 1-1 Strategic approach to HRA method development

1.1.4 Scope of IDHEAS General Methodology

Because IDHEAS-G is an application-independent HRA methodology, it can be used for nuclear and non-nuclear related HRA contexts. For nuclear-related applications, the methodology is applicable to the broad context of human performance for NPP safety shown in **Error! Reference source not found.**.

Table 1 HRA application areas

Dimension	Specifics
Plant Mode	• At-power • Low power and shutdown
Event Type	• Internal • External hazards
PRA Phase	• Level 1 • Levels 2 & 3
Radiation Source	• Reactor • Spent fuel pool • Dry cask storage • Radiation equipment and medicine
Reactor Generation	• Existing reactors • New & advanced reactors
Temporal Phase	• Pre-initiator • Initiator • Post-initiator
Actor	• Control room operator • Control room and local operators • Local operators
Risk-Informed Program	• SPAR • ASP • SDP
Level of analysis	• Detailed • Bounding (screen and scoping)

1.1.5 The intended use of IDHEAS General Methodology

IDHEAS-G includes six elements, as follows:

- Scenario analysis and operational narrative
- Identification of human failure events (HFEs) and feasibility analysis
- Task analysis and time uncertainty analysis
- Basic Quantification Structure
- Development of application-specific quantification models
- Integrative analysis

Three of the elements, scenario analysis and operational narrative, identification of HFEs and feasibility analysis, and task and time uncertainty analyses, comprise qualitative analyses. The Basic Quantification Structure and development of application-specific quantification models are used for HEP quantification. The final element, integrative analysis, integrates the qualitative and quantitative analyses.

The output of each element provides an understanding of human performance at a different level of detail. Depending on the goal and need, an HRA team may choose to perform the full process of HRA defined in IDHEAS-G or only certain parts of it. IDHEAS-G can be used to --

1) Develop an HRA model for a given application in prospective PRA or retrospective risk-informed regulatory activities (e.g., ASP and SDP).
2) Retrospectively analyze a human failure event to understand human performance challenges and identify areas or corrective actions for improving human performance.

1.1.6 The structure of the report and terminology

The subsequent chapters of this document focus on one of the IDHEAS-G elements. The Appendix presents two examples demonstrating the use of IDHEAS-G. In each of the chapters, we describe the objective of the element, present guidance for implementing the process, and describe the expected outputs of performing the analysis defined in the element. Throughout the chapters, many examples and additional information are provided to facilitate readers' understanding of the guidance. These are all taken from the NPP context, but IDHEAS-G can be applied to other contexts.

The terms used in this report are intended to be kept as application-independent as possible, but can be replaced with application-specific terms. For example:

- System – the safety-critical object for operation. It can be a NPP, medical equipment, or any safety-critical machine or computer-based system operated by humans.
- Personnel or operator – An individual that operates the system; this can be a NPP operator, field operator, or technicians.
- Crew – A structured team consisting of multiple personnel each with his or her assigned role and responsibilities.

1.2 Overview of the Methodology

This section provides an overview of IDHEAS-G, with a brief introduction to each of its elements. Table 1-2 summarizes the elements. Typically, a full HRA process goes from Element 1 to Element 6, and the outputs of earlier elements are used as the inputs to later elements. However, there are situations where some elements should be performed iteratively for thorough analysis.

Table 1-2 HRA General Methodology process and outputs

Process step	Outputs of the step
Preparation: Define the HRA issue and analysis scope	Analyst understanding of the issue, project plan, and expected outcomes
Step 1: Scenario analysis and operational narrative	Identification of initial conditions, initiating events, boundary conditions, and consequences of interest (or sequence termination criteria) Description of scenario: Event progression described in timeline or narrative stories or both Scenario context: Plants (systems), crew, and task context

Step 2: HFE analysis – Identification, definition and feasibility analysis	Development of the baseline event sequence and deviation event sequences through "What-If" questions Identification and definition of HFEs HFE feasibility analysis
Step 3 – Crew Response Diagram (CRD), task analysis, error recovery, and time uncertainty analysis	Development of a crew response diagram (CRD) that represents the expected crew response paths along with the detailed timeline of critical responses Identification and analysis of critical human tasks along the CRD Time uncertainties and their contribution to HEP
Step 4: The Basic Quantification Structure	A basic set of cognitive failure modes (CFMs) that represent the full cognitive processes of the four macrocognitive functions (*Detection, Understanding, Decision-making, Action execution*) A comprehensive list of PIFs Cognitive mechanisms that link the CFMs and PIFs
Step 5: Development and use of application-specific quantification model	Selection of CFMs and PIFs pertinent to the application Estimation of HEPs of the CFMs for various combinations of the PIFs (model-based, data-based, or expert judgment)
Step 6: Integration – results review, dependency analysis, and uncertainty analysis	Documentation of model, process, and parameter uncertainties HEPs after review and consideration of dependencies HRA documentation

2 Step 1 - Scenario Analysis and Operational Narrative

2.1 Initial Condition, Initiating Event, and Boundary Condition

The initial condition is the status of the plant (or system) and crew (or single operator) before the initiating event. An initiating event is "an event originating from an internal or external hazard that both challenges normal plant operation and requires successful mitigation." [1]. The boundary condition is the assumptions the HRA and PRA analysts apply to the analysis. An example boundary condition is the assumptions that the HRA team makes about the initiating event's effects on the availabilities of staff and equipment. Having clear definitions of the initial condition, the initiating event, and the boundary condition among HRA team members is important to reduce uncertainty and to facilitate communication between staff with different technical disciplines participating in the analysis.

2.1.1 Initial Condition

The initial condition describes the initial conditions of the plant (or system) and the crew. The description of the initial condition includes the plant or system's operational status, information about the plant or system's configuration at the time of the initiating event and any unavailable components, as well as any other relevant information important to describe the situation preceding the event.

Regarding operational status, PRA models of NPPs typically differentiate among plant operating states, generally defined as at-power, low-power, and shutdown. These operating states are distinguished in the PRA model because the plant responses (e.g., accident sequences) are different in each state and impose different demands on personnel to respond to an abnormal or emergency event. These three states are describe as the following [NUREG-2122]:

- At an at-power state, the reactor is producing a significant amount of power from fission in the core fuel, above and beyond the decay heat levels. The safety systems are on automatic actuation and not blocked or defeated (as they might be in low-power and shutdown states). The support systems are aligned in their normal configuration (e.g., electric power is being drawn from the grid).
- At a low-power state, most safety systems are on automatic actuation but some may be disabled or blocked (e.g., main feedwater trip in boiling-water reactors). The support systems are aligned in their normal configuration (e.g., electrical power is being drawn from the grid).
- In a shutdown state, the core is not producing power (i.e., the reactor is subcritical). The reactor temperature and pressure are lower than at-power, coolant inventory may be lower or higher, the reactor may be relying on alternate cooling systems, some safety systems may be defeated, or containment may be open.

Describing the initial condition also includes specifying the plant's or system's configuration at the time the initiating event occurs and whether any components are unavailable, including any that have failed but the failure has not been detected (i.e., a latent failure). The purpose of this activity is to identify whether the plant has a different configuration in its component lineup for a specific operation that could affect scenario progression following the specified initiating event, including plant and operator responses to the event. For example, are important components unavailable due to maintenance? Are personnel aware that the component is unavailable? The Accident Sequence Precursor (ASP) and the Significance Determination Process (SDP) of the NRC's reactor oversight process (ROP) estimate the increased plant risk (e.g., core damage frequency) from normal condition based on deficiencies in plant configurations (i.e., condition analysis) or the increased risk of a real event (i.e., event analysis such as the NRC's Reactive

Inspection as described in MD8.3/MC-309). The event analysis (e.g., reactive inspection) typically includes the specific plant configuration affecting human response and scenario progression that are not usually included in the base PRA models, e.g., the Standardized Plant Analysis Risk (SPAR) models. For example, in the H.B. Robinson fire event that occurred on March 28, 2010 [ML101830101], jumpers had been incorrectly installed and the error had not been detected. As a result, the expected automatic swap of charging pump suction from the volume control tank (VTC) to the refueling water storage tank at low VTC level did not occur. This latent failure was identified in the SDP and ASP analysis because the initial condition significantly affected the available time for the operators to prevent a reactor coolant pump seal loss of coolant accident.

Example *- In the H.B. Robinson fire event occurred on March 28, 2010 [ML101830101], incorrect jumpers installation caused the automatic swap of charging pump suction from the volume control tank (VTC) to refueling water storage tank (RWST) at low VTC level did not occur.*

It is also important to define or identify the number of available personnel and their skillsets. Lack of sufficient manpower or needed skillsets could increase the likelihood of failure. For example, in NEI 12-06 "Diverse and flexible coping strategies (FLEX) implementation guide," an IC for performing the analysis for an extreme external event is that the on-site staffing level at the time the event occurs is at the site administrative minimum shift staffing level. This initial condition combines with a boundary condition of no site accessibility within the first six hours after the event and highlights that the staffing level (and skillsets) may be an important HRA factor for certain events.

In a phased analysis, the initial condition of a subsequent phase is defined by the results of the previous phase. For example, a common level-2 PRA practice is to use a bridge event tree to group the Level-1 cut-sets based on the plant configuration at the time of core damage. Each cut-set group represents a specific plant damage state (PDS) which in turn is the initial condition of a Level-2 event tree (containment event tree). The grouping reduces the analysis efforts but it may not carry certain key information needed for Level-2 analysis. If the effects are deemed significant the bridge event tree should be revised to distinguish the differences.

Example - *The core cooling availability (available or failed) is a factor in the bridge trees to group the cut-sets. At the time of core damage the core cooling may not be available. But the portable (FLEX) equipment could become available or the core cooling system was repaired after the core damage to provide core cooling to reduce the radionuclide release to outside environment that usually take many hours occur. Another consideration is whether the unavailable core cooling is due to hardware failure or human failure. This could affect inclusion of the task dependency into the calculation of human error probability (HEP) in the containment event tree.*

There may also be additional information about the circumstances preceding the event that is important to specify. For example, if a plant site has more than one operating reactor and the event of analysis affects more than one reactor or spent fuel pool (SFPs), then the characteristics of the initial condition must be specified for each reactor and SFP individually and for the site as a whole to identify the shared resources.

2.1.2 Initiating Event

The ASME/ANS PRA Standard [2] defines an initiating event as "an event either internal or external to that which perturbs the steady state operation of the plant by challenging plant

control and safety systems whose failure could potentially lead to core damage or release of airborne fission products. These events include human-caused perturbations and failure of equipment from either internal plant causes (such as hardware faults, floods, or fires) or external plant causes (such as earthquakes or high winds)."

***Example** - Initiating events can arise from the following:*

- *Internal Hazards, which include:*
  - *Internal event*
  - *Floods*
  - *Fires*
- *External Hazards, which include:*
  - *Floods*
  - *High winds*
  - *Seismic events*
  - *Other external hazards (extreme weather conditions and tornado, etc.)*

These hazards result in different types of initiating events. Examples of initiating events in a NPP are transients and loss-of-coolant accidents.

The terms initiating event and initiator are both used in a PRA context and generally have the same meaning. In some cases, the term initiator may refer to a class of initiators (e.g., transient), while the term initiating event may refer to the actual event (e.g., loss of a feedwater pump resulting in a transient).

***Example -** The initiating event in the SDP analysis of the Monticello Nuclear Generating Plant (MNGP) [3] is a hypothetical external flood event that requires the MNGP to build a levee and bin wall to protect the important component from flood damage. The SDP analysis was initiated because the MNGP was identified failed to maintain an adequate flood procedure with the means to support the timely implementation of a required flood protection feature. This deficiency would affect plant safety in the hypothetical flood,.*

2.1.3 Boundary Condition

The boundary condition is the assumptions applied to the analysis that need to be satisfied. Clearly specifying the boundary condition for the analysis reduces uncertainty in the analysis and facilitates communication between analysts from different technical disciplines. If relevant to the analysis, the boundary condition should include general information (e.g., reactor type and containment type) and plant- or system-specific information (e.g., unique plant system and unique plant configuration).

***Example -** The following Nuclear Energy Institute (NEI) guidelines provide an example boundary condition for performing a PRA for an extreme external event-induced initiating event of extended loss of all ac power (ELAP) and loss of ultimate heat sink (LUHS).*

- *NEI 12-01 "Guideline for assessing beyond design basis accident response staffing and communications capabilities" [4] establishes the site accessibility, staffing, and communication equipment boundary conditions.*
- *NEI 12-06 "Diverse and Flexible Coping Strategies (FLEX) Implementation Guide" [5] describes initial conditions and the conditions immediately after the initiating event.*
- *NEI 13-06 "Enhancements to emergency response capabilities for beyond design basis accidents and events"[6] addresses the training personnel will have at the time of the event.*

- *NEI 14-01 "Emergency response procedures and guidelines for beyond design basis events and severe accidents" [7] specifies the procedures and guidelines that will be available to personnel and their development and maintenance.*

Example – *The following list the general boundary condition in NEI 12-06 for the analysis of beyond-design–basis external events:*

- *Beyond-design-basis external event occurs impacting all units at the site.*
- *All reactors on-site are initially operating at power, unless the site has procedural direction to shut down due to the impending event.*
- *Each reactor is successfully shut down when required (i.e., all rods inserted, no ATWS).*
- *On-site staffing is at the site administrative minimum shift staffing levels.*
- *No independent, concurrent events are occurring, e.g., no active security threat.*
- *All personnel on-site are available to support site response.*
- *Spent fuel in dry cask storage is outside the scope of FLEX.*

Example – *The following describe a specific boundary condition example in NEI 12-01 for the analysis of beyond-design–basis external events regarding site accessibility:*

- *No site accessibility within the first six hours, i.e., all of the onsite tasks must be performed by the personnel at the site when the event occurs. The number of available personnel is further limited to the minimum staffing for emergency response.*
- *Limited site access before 24 hours, i.e., offsite personnel are assumed to begin arriving at the site to support event mitigation but offsite equipment is still not available.*
- *Site is accessible after 24 hours, i.e., both offsite personnel and equipment are available at the site to support event mitigation.*

Example -*The ASP and SDP analyze plant risk associated with a specific plant condition or plant event. Because of their retrospective nature, the boundary condition would be specific to a finding (a condition). For example, the SDP analysis of the Monticello Nuclear Generating Plant (MNGP) [3] was about a finding that the MNGP failed to maintain an adequate flood procedure with the means to support the timely implementation of a required flood protection feature. The boundary condition was that the plant did not have a flood procedure available to respond a hypothetical flood event. This boundary condition led to the determination that site would not be able to build a barrier in time to prevent the hypothetical flood in the SDP analysis.*

2.2 Develop the Baseline scenario

2.2.1 Scenario narrative and timeline

The purpose of developing the baseline scenario is to delineate the expected plant and human responses under the initial condition, initiating event, and boundary condition assumptions. The characterization of plant-human interactions within the scenario is developed from the operator trainers' perspective for NPP analyses. In developing the baseline scenario, except for what is specified in the initial condition, initiating event, and boundary condition, it is assumed that there are no additional hardware failures and the operators respond to the event as they were trained. The main purpose of developing the baseline scenario is for the HRA analysts to have an in-depth understanding of the scenario. This understanding will permit the analysts to analyze the event from the operator's perspective and informs them of potential instrument and system control settings and operational limitations that may affect the operator's responses and scenario progression.

Information such as key automatic system responses, procedures transitions, human actions, key operational considerations, e.g., system limitations, task priorities, task dependencies, and action timing, etc. is useful to include in the baseline scenario documentation. The baseline scenario documentation includes two elements:

- A description of the scenario at an appropriate level of detail to understand the scenario progression. The purpose of this scenario description is to understand the flow of the human-system interactions during the course of the scenario, but does not describe the details of how each human task is performed. The task details (task analysis) are discussed in the crew response diagram (CRD) section of this report.
- Inclusion of operating experience related to the scenario, if applicable. It is a common practice of nuclear power plants to include operating experience in their simulator training document. Operating experience is also frequently used in plants to raise awareness of plant safety. Even though it is not a requirement when developing the baseline scenario, it is a good practice for the HRA analysts to search for operating experience related to the scenario.

In developing the baseline scenario, it is recommended to present the scenario in chronological order. The two columns timeline format (such as in the NRC's augmented inspection reports), with one column showing the date/time information and the other column showing all other information, is a common timeline documentation practice. The following guideline improves the two-column timeline format by maintaining similar flow and simplicity with added information and information classification to improve the readability and to support HRA:

- Describe the initial condition, initiating event, and boundary condition of the scenario at the beginning of the timeline.
- Use a two-column timeline format as described below:
    - Column 1 - Date and time. For convenience of analysis, set time zero at the time the initiating event occurred. So the time in Column 1 of the timeline items represents the lapse of time from the initiating event (time zero). For analyzing real event that has occurred (i.e., SDP and ASP event analyses), the local date and time of the time zero should be provided.

      Example – *The H.B. Robinson fire event occurred on March 28, 2010, the electric fault caused a fire event occurred at 18:52. The time zero is 18:52, March 28, 2010 (local date/time). The date could be informative in respect to human performance especially if the event occurred during a holiday or weekend. In this case, March 28, 2010 is Sunday.*

      If incidents occurred before the initiating event that provide useful background information to support the HRA, the incidents should be indicated in the timeline. Use negative time or exact time (e.g., -3 days or 2/3/2010) in column 1 for the incidents that occurred before the initiating event.

      Example - *Before the H.B. Robinson fire event occurred on March 28, 2010, the crew composition was unusual because the site was preparing for the upcoming refueling outage. The Shift Supervisor (SS) was a staff crew rather than an operation crew. The staff crew only needs to fulfill the minimum watch-standing requirement to maintain their operating licenses. In addition, at the time of the reactor trip, the main control room (MCR) was manned with a shift supervisor, a reactor operator and a balance-of-plant operator. The shift manager and shift technical advisor were at a pre-shift turnover meeting with the previous crew in another room a couple minutes' walking distance from the MCR and with the*

telephone line connected to the MCR. This information should be included in the initial condition discussion.

- Column 2 – Human-system interactions related information. The information is classified into four types to improve understanding of the human-system interactions. Each information type is denoted by a different bold letter as described below:
  - System or plant automatic responses **(S)**: The **S** indicates that the information is a system and component automatic response. These responses are based on the automatic settings therefore no human actions are needed to generate these responses. An example response is automatic safety injection due to low pressure in the reactor coolant system (RCS).
  - Plant status information **(I)**: The **I** indicates that the information is system or plant information indicating an important threshold has been exceeded. Examples are alarm actuations and steam generator water level reaching the main steamline level.
  - Human responses **(H)**: The **H** indicates that the information is related to human response. It includes the human's physical actions to interact with the system and the information that leads to the human actions. Example information includes:
    - The cue(s) that initiated the human cognitive process and eventually led the individual to interact with the system to change the scenario course. The information could be alarms or specific human actions and the cue(s) to enter or exit a procedure.
    - The human actions (e.g., depressurize the RPV using SRVs) and the basis of the human actions (e.g., procedure-X, step-Y).
    - The procedure transitions and the basis of the transitions (e.g., transfer from E-0 "reactor trip procedure" to E-3 "Steam Generator tube rupture procedure" based on satisfying the E-0 Step-X's transition criteria).
    - The principal person affected by or performing the above responses. For example, shift supervisor enters E-0 due to a reactor trip, and the shift technical advisor enters the critical safety function tree because the CSFT entry criteria are reached. If the human response is not associated with a single job role, use "crew" as the principal person. For example, detecting a pump trip indication is the responsibility of all crew members in the MCR.

  - Notes **(N)**: This column is used to provide additional information regarding the specified plant responses and human actions. The following are example **Ns**:
    - System automatic actuation set point or actuation logics
    - Component operation limitations, e.g., Operating the safety relief valves requires dc power and pneumatic pressure
    - Specific human action considerations, e.g., cooldown RCS at a rate not greater than 100 °F/hr
    - The action requires special equipment or a vehicle, etc.

- The operational considerations, e.g., interferences with the concurrent tasks.

Example – *A timeline example is presented in section 2.2.2.*

2.2.2 Operating Experience

The HRA analysts are encouraged to include operating experience related to the event of analysis. Inclusion of operating experience in the operator simulator training scenarios is a common practice to raise operators' awareness of the potential issues. The operating experience could be operating experience of the similar events or operating experience of performing similar tasks, e.g., swapping RCS cooling from injection to sump recirculation. The operating experience shows human responses, including human successes and human errors, in real events. The information is helpful for HRA analysts to have better appreciation of the human responses in real events of similar conditions.

Example – *Table 1-1 is a timeline example for a beyond-design-basis earthquake that caused a combination of an extended loss of AC power (ELAP) event and a loss of ultimate heat sink (LUHS) event. Only part of the scenario is presented in table 1 because the main purpose is to illustrate the timeline information discussed in section 1.2.1 and 1.2.2.*

Table 2-1 An example timeline

Reactor type: GE Type 4 BWR; Mark 1 containment in a dual reactor site **Initial condition:** Both reactors are at full power operation. Plant staffing is at the minimum emergency operation level. **Initiating event:** a beyond design basis (BDB) earthquake caused an event of extended loss of ac power (ELAP) and the loss of ultimate heat sink (LUHS) due to failure of the downstream dam. **Boundary condition:** The earthquake caused site wise damage but the seismic class robust structures remain intact. No personnel injury. All onsite personnel are able to respond to the event. No site access is available within the first six hours following the earthquake. More detailed boundary condition information can be found in NEI 12-06 [ML].	
Time (hh:mm)	**Human-System Interactions Related Information** **S:** System automatic responses **H:** Human responses **I:** System or plant status information, e.g., alarms and indications. **N:** Analysts' notes
00:00	**S:** An ELAP event and a LUHS event occurred due to a BDB earthquake. **N:** Assume the main ground motion lasts for five minutes.
00:00+	**S:** Reactor Scrammed & Turbine tripped **S:** HPCI[1] and RCIC[2] start automatically on -48 inch signal. **I**: Many alarms in the alarm panels were triggered. **N**: HPCI/RCIC actuation is an approximation – depending on how the event is initiated, RCIC could start automatically or be manually started by the operator.
00:05	**H(SS):** Enter RPV[3] control procedure (based on reactor scram) **H(SS):** Enter SBO[4] procedure based on no offsite power and no EDG[5] loaded. **H(RO):** Shutdown HPCI

[1] HPCI: High Pressure Coolant Injection
[2] RCIC: Reactor Core Isolation Cooling
[3] RPV: Reactor Pressure Vessel
[4] SBO: Station Black Out
[5] EDG: Emergency Diesel Generator

	H(Crew): Call the onsite operators to report to the MCR **N:** Because there is no indication of a LOCA[6] event, as long as RCIC is in service, HPCI operation is not required. Shutdown HPCI to conserve dc power.
00:15	**H(MCR):** distribute master keys in MCR to onsite operators **H(EO[7]1):** Shed dc load per procedure X, attachment A (45 min[8].) **H(EO2&3):** Locally start the EDGs per procedure X, attachment B (45 min.). **H(RP[9]):** Establish backup N_2 per procedure Y (30 min.) **H(SSD[10]):** Conduct site assessment per procedure Z **H(SM):** Declare a site area emergency based on EAL XX (SBO) – mobilize the emergency response organization **N:** The dc load shed is performed at the cable spreading room, reactor building and turbine building. **N:** Backup N_2 cylinders are within the reactor building.
00:20	**H(RO):** Open SRVs to cooldown and depressurize RPV. Reduce pressure to 500 psi, then 100 °F/hr rate to between 200 and 300 psi. (two hours)
01:00	**H(SM)**: Declare a general emergency based on EAL YY (ELAP) **H(SS):** Enter ELAP procedure due to no ac power is expected to be restored within 1 hour after the ELAP.
…	

Operating Experience [the National Diet of Japan "The official report of Executive summary, The Fukushima Nuclear Accident Independent Investigation Commission]: On March 11, 2011, the Great East Japan Earthquake triggered an extremely severe nuclear accident at the Fukushima Daiichi Nuclear Power Plant (NPP), owned and operated by the Tokyo Electric Power Company (TEPCO). When the earthquake occurred, Units 1, 2, and 3 of the Fukushima Daiichi plant were in at-power operation; and Units 4 to 6 were undergoing periodical inspections. The emergency shut-down feature, or SCRAM, went into operation at Units 1, 2 and 3 immediately after the commencement of the seismic activity. The seismic caused a loss of the offsite power to the Daiichi NPP. The emergency diesel generators (EDGs) automatically started as designed. The tsunami caused by the earthquake flooded and totally destroyed the emergency diesel generators, the seawater cooling pumps, the electric wiring system and the DC power supply for Units 1, 2 and 4, resulting in loss of all power—except for an external supply to Unit 6 from an air-cooled emergency diesel generator at about 50 minutes after the earthquake. In short, Units 1, 2 and 4 lost all power; Unit 3 lost all AC power, and later lost DC before dawn of March 13, 2012. Unit 5 lost all AC power.

The tsunami did not damage only the power supply. The tsunami also destroyed or washed away vehicles, heavy machinery, oil tanks, and gravel. It destroyed buildings, equipment installations and other machinery. Seawater from the tsunami inundated the entire building area and even reached the extremely high pressure operating sections of Units 3 and 4, and a supplemental operation common facility (Common Pool Building). After the water retreated, debris from the flooding was scattered all over the plant site, hindering movement. Manhole and ditch covers had disappeared, leaving gaping holes in the ground. In addition, the earthquake lifted, sank, and collapsed building interiors and pathways, and access to and within the plant site became extremely difficult. Recovery tasks were further interrupted as workers reacted to the intermittent and significant aftershocks and tsunami. The loss of electricity resulted in the sudden loss of monitoring equipment such as scales, meters and the control functions in the central control room. Lighting and communications were also affected. The decisions and responses to the accident had to be made on the spot by operational staff at the site, absent valid tools and manuals.

[6] LOCA: Loss of Coolant Accident

[7] EO: Equipment operator

[8] Action time.

[9] RP: Radiation protection

[10] SSD: Safe shutdown technician

2.2.3 Interaction with other disciplines to develop the Base event timeline

A risk analysis team may include personnel from multiple technical disciplines. For example, the technical disciplines for a reactor safety analysis could include plant simulation analysts (performing MELCOR simulation), PRA analysts (developing event sequence models), consequence analysts (Performing MACCS calculations), HRA analysts, an NRC plant project manager (who has in-depth knowledge about the plant's systems and configuration), and the study-specific discipline analysts (e.g., seismologist, system analysts, and operators). The PRA provides the framework to integrate the knowledge of different disciplines to assess risk.

Traditionally, the PRA analysts would perform detailed event-sequence analysis (using techniques such as event sequence diagrams) to illustrate all possible success paths from the specified initiating event leading the system (reactor) to a desired state (e.g., reactor is in safe-shutdown or safe-stable state). In this context, regarding teamwork, the PRA Procedures Guide [NUREG/CR-2300] states,"The event sequence diagram tends to include a significant amount of design and operational information relative to the potential success paths. Their construction is an iterative process with input from various PRA team members, particularly those who have transient analysis, operational, and simulator experience." An emphasis is that the team interaction is an iterative process throughout the study.

Regarding team interaction, the HRA analysts should consult the individuals who have operating experience or are familiar with operation of the study subject (e.g., same type of reactor, spent fuel maneuver, and radiation medical device) to develop a draft baseline scenario. The draft baseline scenario then is refined with input from the other disciplines such as PRA assumptions, the system responses and timing generated from plant simulation, and system operating characteristics and constraints identified by the system analysts. This iterative interaction ensures the final baseline scenario is consistent with other disciplines' assumptions and results. As a whole, this process improves the quality of the final results. To the HRA analysts, this process provides opportunities to have a holistic and in-depth understanding of the scenario. This understanding is essential to improve the analysts' sensitivity in identifying human performance vulnerability in the scenario for more reliable scenario modeling and human reliability estimates.

2.2.4 Good practices in baseline scenario development

The following is the general process of developing a baseline scenario. Even though they are listed sequentially, these steps are iterative until the final baseline scenario is developed:

1. Clarify the initial condition, initiating event, and boundary condition: At the beginning of the study, communicate with the other team members to ensure that a consistent initial condition, initiating event, and boundary condition are applied to the study. Each discipline may have a discipline-specific initial condition, initiating event, and boundary condition. This should not affect consistency of the overall analysis.
   Example – *In an event resulting in the SRVs cycling to maintain RPV pressure, a common boundary condition imposed by the PRA or system simulation is that the SRV would fail open after a certain number of cycles. The boundary condition changes the scenario transitioning from high RPV pressure to uncontrolled rapid RPV depressurization that, in turn, affects the operator's responses.*
2. Identify HRA-specific boundary condition: The boundary condition is what can be assumed with certainty will occur in the event. Boundary condition specifies the assumptions applicable to the whole event tree. The event tree's top events are additional assumptions applied to portion of the event tree. HRA analysts should identify the HRA-specific BCs, either for the whole or partial event tree. Examples of HRA-

specific BCs are the site accessibility constraints and staffing levels specified in NEI 12-06 for responding to BDB external events.

3. Develop a draft baseline scenario: The applicable operating procedures, if available, provide a good basis for developing a draft baseline scenario, in addition to consulting with individuals who have operating experience or are familiar with the operations of the plant or system of interest. Include the estimated time and the reasons for each important human action and procedure transition. The reasons should be consistent with operator training and procedure instructions. Useful supplemental information, if available, includes the procedure technical basis documents, the final safety analysis report (FSAR), and operator training material.

   The ASME/ANS PRA Standard Requirement HR-E1 [2] *"when identifying the key human response actions REVIEW (a) the plant-specific emergency operating procedures and other relevant procedures (e.g., AOPs and ARPS) in the context of the accident scenarios and (b) system operation such that an understanding of how the system(s) functions and the human interfaces with the system is obtained."*

4. Refine the baseline scenario: Interact with the PRA analysts and the system simulation analysts (e.g., MELCOR analysis) to revise the draft baseline scenario, which may include adjustments to the scenario course and system response timing. Present the information in the timeline format.

In developing the baseline scenario, the HRA analysts should collect information to identify other scenarios to be modeled in the study. The following is additional information that will support the identification of the other scenarios (discussed in section XX):

- Identify the component operational constraints: The active system and components need a driving force to operate, e.g., electricity (ac or dc power), pneumatic pressure, steam pressure, etc. The scenario may disable or significantly reduce the system and component availability by reducing or eliminating the driving force.
  Example – *During a station black out (SBO) event, the BWR operator uses the safety relief valves (SRVs) to depressurize RPV, and the PWR operator uses the atmospheric relief valve (ARV) or SG Power Operated relief valve (PORV) to depressurize the SGs and RCS. Operating these valves typically require dc power and air pressure. Both sources are limited in an SBO event. The dc power will be depleted in a few hours if the battery is not charged in time. Air pressure is provided by pressurized air bottles that only have enough air to operate the valve for a limited amount of time. Without connecting to a larger air source, the valves cannot be used to depressurize RPV or RCS after a few depressurization cycles.*
- Task performance characteristics: Take notes on the following information:
  - task implementation location (MCR and local)
  - procedure to implement the task
  - number of personnel and skillset required
  - special equipment and vehicle needed
  - task validation records (for action time information)
  - potential task interference (e.g., sharing the same resource with the other concurrent tasks) and task dependency (e.g., tasks have to be performed in sequential order, such as obtaining external permission to perform the task).
- Observe operator simulator exercises or event drills, if available, to confirm and revise the baseline scenario. **"**While a walkdown of the control room and observations of simulator exercises and talk-throughs with crews about various accident scenarios are probably most important during the modeling phase, if time and resources allow, they

may also be useful during the identification phase to help analysts understand the procedures and how they are implemented by the crews" [NUREG-1792 HRA Good Practices].
- Review and document the operating experience related to the scenario, if available, to understand factors that complicated the situation in past events.
- 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. [NUREG-1792 HRA Good Practices]

Since of the publication of WASH-1400 [8] in 1975, PRA modeling has become much more brief and efficient after more than four decades of improvement. It is more likely that a new PRA model will be developed by modifying existing PRA models instead of developing the new model from scratch. Therefore, the draft PRA event tree will likely be developed before the HRA baseline scenario is developed. In this case, HRA analysts still need to develop a detailed baseline scenario. A potential benefit is that the HRA analysts may identify key human actions overlooked by the PRA analysts. These human actions are unlikely to be identified without going through the detailed baseline scenario construction process.

For the SDP and ASP event analyses (i.e., the change in plant risk of an event that has occurred), the baseline scenario is the actual scenario of the event rather than the expected scenario. The relevant disciplines likely include the operating crew in the event, operator trainers, and NRC inspectors. These individuals can provide valuable information for the HRA analysts to reconstruct the baseline scenario.

2.3 Context analysis

Human performance is dependent on the nature of the task and the conditions in which the task is performed. The objective of the context analysis is to document significant challenges to human performance; these challenges provide the basis to estimate the HEPs of the HFEs of interest. Typical challenges are grouped into three groups:

- The scenario (the event and evolution)
- The crew who performs the task
- The tasks to be performed

The condition of any above group could affect human performance. For systematic analysis, the influences on human performance are represented by factors (context factors) in the IDHEAS-G methodology. Sections 1.3.1 to 1.3.3 discuss the substance of the scenario context, crew context and task context, respectively. This guidance provides a set of performance influencing factors (PIFs) associated with the three types of contexts. The overall that affects human performance is characterized by the statuses of the PIFs.

2.3.1 Scenario Context

The scenario context provides a birds-eye view of the scenario for a holistic understanding of the scenario progression before diving into the details analysis of a specific HFE. The scenario context should include the following elements:

- Initial plant conditions, including operating conditions of all the units on the site, initiating events, and latent failures

- Expected important structure, system, and component (SSC) responses. Pay special attention to the systems, which, if they fail, would significantly challenge plant safety. This typically is the plant safety systems and components, and the defense-in-depth barriers to a radioactivity release from fuel, RCS, and containment.
- The conditions that challenge the SSC functions mentioned in the previous bullet including support systems, ancillary functions, and the concurrent activities to protect workers or major equipment (e.g., vent hydrogen from the main generator in certain events).
- Key operator actions (inside and outside of the main control room) and timing during the scenario progression
- Communications with offsite supports
- Component behavior and the limiting factors of operation
- Effects of system and human failures

2.3.2 Crew context

The crew context is the characteristics of the situation that affect crew responses. This includes the information, stimuli, and conditions that influence the crew to perceive information related to the plant abnormality, understand the situation, make correct decisions, and perform the required actions in time to prevent an undesired consequence from happening. In a team environment, factors affecting human performance are grouped into the following four macrocognitive functions:

- Detection (of information)
- Understanding (the situation)
- Decision-making (of how to respond to the situation)
- Action execution (to implement the planned responses to achieve the desired of goals)

Identification of operational challenges should be based on an understanding of how the four macrocognitive functions are performed. The operational challenges are the factors that can fail the macrocognitive functions. Because the macrocognitive functions could be performed in a teamwork environment, the teamwork element should also be considered in analyzing each macrocognitive function. The following provides more discussion of the four macrocognitive functions and teamwork.

The Crew context describes the conditions that could significantly affect the macrocognitive functions. The following are the general areas of consideration for the Crew context:

- Activities other than controlling the plant – High-level ongoing activities that the full or parts of the crew may be involved in, such as multi-unit events, emergency evacuation, on-going maintenance.
- Work site accessibility – Whether the required personnel and equipment can reach the work site using the specified travel routes.
- Adverse environment – Environmental considerations, such as fire, smoke, flood, earthquake, noise, illumination, temperature extremes, and high radiation, can affect the performance of the macrocognitive functions.
- Information availability and reliability – including information completeness, reliability, and whether information is presented timely. For example, computer systems may become temporally unavailable, some sensors or indicators may become unreliable.
- Availability and applicability of procedures, instructions, and guidance documents –The procedures and guidance provide instructions to assist the operator to complete the tasks. The procedures' applicability (to the scenario), quality (e.g., have been simulator validated), and granularity (providing the right level of detail) are to be considered.

Things such as whether the required human responses have procedures, whether the procedures match the responses, whether the procedures cover the necessary details of the response or there are skill-of-the-craft actions, etc. are examples of practical considerations.

- Decisions and decision-makers – It is generally assumed that the shift supervisor in the MCR is the decision maker. Yet, some scenarios may require decisions beyond the MCR personnel such as STA, the Technical Support Center (TSC), emergency response centers, and various authorities. A lack of availability of such decision-makers and the infrastructure of decision-making can impose challenges to human actions.
- Staffing and skills - In responding to extreme external events, the staffing level may be marginal to complete the necessary tasks within their specified time. For example, NEI 12-01 assumes that an unspecified beyond design basis external event will cause the site to be inaccessible to offsite personnel within the first six hours after the event. Applying an additional assumption that the onsite staff is at the emergency plan minimum staffing level, this combination could challenge whether the site has sufficient personnel with required knowledge and skills to complete all required tasks before the offsite personnel become available. In addition to staffing level and skills, the coordination infrastructure may impact the effectiveness and efficiency of staffing.
- Training – Training is essential to ensure that the individuals have the required knowledge and abilities to perform the task. Inadequate training such as long training interval or no training on human or system failure modes could significantly challenge performance. For example, in simulator training, the crew typically is trained to respond to the scenario with a single failure at a time. The crew is trained less thoroughly on responding to scenarios with multiple simultaneous failures. The HRA benchmark studies show that if simultaneous failures have similar or counter-effects on plant symptoms, the scenarios are cognitively challenging to the operators.
- Equipment availability– Equipment refers to hardware that is needed to perform tasks. This could include special equipment, tools, parts, and keys (to unlock the normally locked component). Equipment availability, transferability, reliability, operability (installation, calibration, testing, and maintenance) are examples that may challenge human performance.
- In addition to the elements listed above, analysts are encouraged to identify and document any other potential challenges to human performance in the scenario.

2.3.3 Task context

Task context refers to aspects of human tasks that challenge performance. The following elements should be considered in the task context:

- Unfamiliar / unusual scenarios – Handling unfamiliar scenarios requires complex and sustained cognitive activities. Unfamiliar scenarios typically impose challenges for crews to understand the situation and make the right decisions. In addition, operator responses could be slower and with greater uncertainty for unfamiliar scenarios compared to familiar scenarios. In unfamiliar scenarios, the situation-specific tasks may not be explicitly identified in the procedures but rather rely on engineering judgment.
- Multitasking – Multitasking refers to performing parallel and intermingled cognitive activities. Because each task requires multiple cognitive functions, such as detecting cues/parameters, comparing and assessing information, programming and executing sequences of actions, operators have to frequently switch between these tasks for multitasking. Frequent switching of cognitive functions is error prone. A typical example of multitasking is that the crew implements concurrent procedures and procedure

attachments in parallel to the main procedures; an extreme example of multitasking is that decision-makers have to handle several units that are under different critical situations.

- Frequent or persistent distraction and interruption – Distraction and interruption refer to non-critical or non-procedural tasks that are added to operators while they are performing critical tasks. Examples of distractions are answering phone calls, being requested to provide information, being distracted by other things going on in the work environment. High distraction / interruption refers to situations in which operators are distracted/interrupted for a prolonged period of time (e.g., longer than 2 minutes) or interrupted by cognitively demanding tasks and requests.
- Unpredictable dynamics – This refers to a situation where system responses differs from what is expected by the crew and procedures (scenario-procedure mismatch), or in a fast-paced scenario where the scenario could include significant changes in a short time that require the operator to constantly monitor parameters and respond promptly. In some situations, the operators may need to monitor multiple parameters, perform mental calculations or simulations to have a holistic understanding of the situation and choose appropriate responses.
- Time pressure and other stresses – Time pressure refers to the sense of time urgency perceived by an operator to complete a task. This sense of time urgency creates a psychological pressure (time pressure) affecting the operator's responses, such as making trade-offs between thoroughness in performing the task and completing the task in time. Because time pressure is based on the operators' perception and understanding of the situation, it may or may not truly reflect the actual situation. Therefore, time pressure is most likely to occur when there is marginal time or inadequate time available, although it also could occur in scenarios with luxury or adequate available time if the individuals have an incorrect understanding. Other stresses, such as concern for families in emergency conditions, potential consequences of plant damage, and personnel safety can also impact performance.
- Mental fatigue – Mental fatigue can be caused by working long, non-routine, stressful hours, or performing unfamiliar, cognitively demanding tasks right after a high cognitive workload period. Mental fatigue leads to loss of vigilance, difficulty in maintaining attention, and reduced working memory span. Humans tend to use heuristics (short-cuts) in situation assessment and decision-making.

Together, the operational narrative and scenario context documented in Step 1 of IDHEAS-G set up a basis for further detailed analysis. For examples, the scenario timeline is the basis for developing the event tree and identifying human failure events (HFEs); the scenario context is the basis for assessing HFE feasibility, time uncertainties, and performance influencing factors (PIFs). As the method progressively decomposes a scenario into HFEs, critical tasks, and PIFs, the operational narrative and context hold pieces of information together to form a logical representation of the entire scenario.

3 Step 2 - HFE Identification, Definition, and Feasibility Analysis

The human failure events (HFEs) are the human actions modeled in PRA models. The objective of Step 2 in IDHEAS-G is to identify HFEs, describe the key features of the HFEs, and assess their feasibility. Step 3 "CRD and Task Analysis" in IDHEAS-G will perform detailed analysis of the feasible HFEs. Step 2 and Step 3 are expected to be performed iteratively. The HFE definition in Step 2 provides the success criteria for detailed analysis in Step 3, while the HFEs identified in Step 2 may need to be merged, split, or re-defined through the detailed analysis in Step 3. Also, an HFE that is initially assessed as feasible in Step 2 may be reclassified to infeasible based on the detailed analysis performed in Step 3.

3.1 HFE Identification

3.1.1 Identify HFEs from the baseline scenarios

The ASME/ANS PRA Standard [2] defines an HFE as "[a] basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or inappropriate action." The human inaction and inappropriate action in the HFE definition are typically referred as an error of omission (EOO) or an error of commission (EOC), respectively. The identification of the candidate HFEs is based on the baseline scenario developed in the previous step and the identification of additional scenarios to be discussed later. After the candidate HFEs are identified, the HRA analysts should work with the PRA analysts to generate a set of HFEs to be modeled in the PRA. The baseline scenario could contain many human-system interactions. It is desirable to reduce the scope of those that need to be studied as early as possible in the process. The objective is to limit the number if human interactions to be addressed without eliminating any potentially important ones. [SHARP 1]

The following human actions should be enlisted as candidate HFEs:

<u>Actions on safety functons</u>

The general PRA principal to identify the event tree's top events (including the HFEs) are based on a hierarchy of plant safety functions, the safety systems (to the plant safety functions), and the sub-systems and components (for the operation of the safety system). Any human actions that directly affect the safety functions should be identified as candidate HFEs.

Example – *The BWR safety functions for core and containment include:*

- *Reactor subcriticality*
- *Reactor coolant system overpressure protection*
- *Early core heat removal*
- *Late core heat removal*
- *Containment pressure suppression*
- *Containment heat removal*
- *Containment integrity*

The systems to control reactivity (subcriticality) include the reactor protection system, standby liquid control, and alternate control rod insertion.

PRA procedures guide actions

The PRA Procedures Guide [9] identifies the following three types of actions to be modeled in PRA ETs:

- The system failure affects the outcome (e.g., plant damage state, radionuclide release, containment response)
  Example - *In a steam generator tube rupture (SGTR) event, the manual actions to cool down and depressurize the reactor coolant system (RCS) prevent the RCS coolant from leaking to the outside environment (via the SG and safety relief valve). Therefore, the action to depressurize and cool down the RCS is a candidate HFE for the SGTR event.*

- The operation of the system contributes to a safety function in this context
  Example – *Failure to manually transfer the safety injection water source to sump recirculation mode before the depletion of the injection water source would result in failure of the safety injection.*

- The operation of the system at this point affects the need, or the operation of, other systems.
  Example – *Failure of a support system (e.g., component cooling water system) or the instrumentation air system in certain scenarios could affect other systems.*

Other actions

In addition, the following actions are good HFE candidates:

- inappropriate or missing human actions could result in phenomena that significantly complicate or prolong event recovery.
  Example - *Inappropriate water injection into a hot core could result in hydrogen burns or detonation to complicate event mitigation.*
- the actions that are necessary to bring the system to the desirable end state (e.g., the reactor in a safe-stable state) or to terminate the event, even if the actions are procedure-guided actions or skill-of-the-craft actions.
  Example - *A key human action in the ASP analysis of the H.B. Robinson fire event on March 28, 2010 is to either restore the RCP seal cooling or restore the degraded RCP seal injection in time to prevent RCP seal failure (a PRA IE).*
- the manual actions to fail or otherwise defeated automatic responses
  Example – *The feed-and-bleed manual action is required to provide RCS cooling in the event that the AFW pumps fail to automatically inject water into the RCS after the main feedwater pumps trip.*

It is helpful to use action words such as actuate, initiate, isolate, terminate, control, change, etc. so that the desired actions are clear [NUREG-1792].

3.1.2 Identify Additional Event Sequences

In addition to the base event sequence, there may be additional event sequences for the basic PRA event, and those sequences may involve additional HFEs. Additional event sequences should be identified by asking "what-if" questions to the basic PRA event tree: "What if the top event failed?" The failure branches generate new event sequences. The analysts ask what if the structure, system and component failures and human failures of the scenario/sequence to identify the new event sequences. Failure of a top event creates a new situation affecting scenario development. This may requires modeling additional structure, system, and component failures and human failures not modeled in the base event sequence. This process

continues until the event tree is fully developed. In a PRA study involving multiple disciplines, a draft event tree that has multiple event sequences may be already developed by PRA analysts. In this case, the draft event tree provides basic guidance for the HRA analyst to analyze each event sequence for its consistency with procedures, operator training, and plant simulation, if available.

The subjects of the what-if questions should only be the component failures and human action failures that directly challenge the key plant functions to mitigate the event. The what-if questions at this point in the analysis should not address factors that may affect component and human performance. For example, a critical human action in a SGTR event is to isolate the broken SG. An appropriate what-if question is "What if the broken SG is not isolated?" To isolate the broken SG, the operators must detect the SGTR symptoms. An important symptom is the actuation of the main steam line radiation alarm. The question about the alarm (What if the radiation alarm failed?) would lead to the identification of the critical action, which is isolate the broken SG(s). The purpose of this step is to populate the event sequences to support the PRA event tree development. The branches' probabilities are to be discusses in a later step.

The analyst's what-if questions in this step should be what if the operators do not perform the desired actions or take inappropriate actions, rather than questioning what factors affect these cognitive functions. The actions to be selected for analysis strongly depend on the interests of the analysis. A consideration is that the action granularity should be consistent among the modeled HFEs and consistent with the HRA method used for the analysis. For example, the following are some human actions modeled in a fire PRA model:

- Operators fail to manually operate a charging pump from the MCR
- Operators fail to close a flow control valve by isolating the air supply
- Operators fail to locally operate a residual heat removal pump when the motor control circuit fails as a result of damage
- Operators fail to restore the steam generator level by locally controlling auxiliary feedwater after damage to the control room indicators
- Operators fail to isolate the power-operated relief valve (PORV) from the control room after it spuriously opens

The same principal applies to asking what-if questions for components and systems. For example, either charging flow or component cooling flow will provide sufficient cooling to protect the seals of the reactor coolant pumps (RCPs). An appropriate what-if question would be "What if the RCP seal failed?" instead of "What if the charging flow is lost?" or "What if there is a loss of component cooling flow?" The latter two questions are modeled in a fault tree.

PRA uses fault trees to represent the logic of the mechanisms that failed in the event tree top events. In some situations, different failure mechanisms (or failure modes) may have significantly different human response considerations. If the differences are significant it would be easier to separate the failure mechanisms (or failure modes) into separate event tree top events. For example, an AFW failure could be a mechanical failure of the AFW pump or depletion of dc power. The AFW pump mechanical failure only affects the AFW system. The dc power depletion has a wide range of effects including instrumentation and control and plant indications. Because of the significant differences in human responses to the two mechanisms of failure, it is cleaner to separate these two failure mechanisms into separate event tree top events.

Some PRA applications may have relevant PRA models already developed. These PRA models can be adopted to use but it may or may not require modifications. Examples are the ASP, SDP, and fire PRA analyses, which start with an event precursor. The event may be developed into an initiating event or a top event of an existing PRA model. It is generally more practical to adopt the existing PRA model (an event tree, likely; and assuming the PRA model is up-to-date) instead of developing a new one. In this case, the HRA analysts should check whether the event precursor (of the SDP, ASP, and fire analyses, etc.) would create the need to modify the existing PRA event tree. This could include removing or adding HFEs to the existing PRA to address analysis-specific considerations.

Examples *– The following two examples are from NUREG-1921 regarding adopting the existing internal event PRA model for fire PRA*

- *The HFE of "operator fails to start a pump after automatic actuation failed" is not always modeled in the internal events PRA because random hardware failures have relatively low failure probabilities for internal events. However, in a situation such as fire, the hardware could be failed by the fire or its reliability severely degraded, such that these operator actions may become important and could be added to the PRA model [NUREG-1921].*
- *For scenarios in which the internal events operator actions are assumed failed because of impacts to the instrumentation or equipment, the HRA analyst may need or wish to credit an additional action. An example of this is an internal event HFE of an operator failing to start a pump. In the internal events model, this HFE is a simple control room action; however, in the fire scenario, the fire fails the control room switch and the HEP evaluates to 1.0. For the fire PRA, the HRA analyst may wish to credit a local action to start the pump. To identify these types of actions, the impact of the fire on the existing internal events actions needs to be known along with the potential success path to be applied. The latter is often identified as a result of operator interviews.*

3.1.3 HFE scope

HFEs are defined for the actions needed to interact with the system, sub-systems or components to change the scenario course. However, because of a lack of explicit guidance on defining the HFE scope in HRA methods, it is observed the HRA analysts vary in modeling HFE in PRA. These differences could affect crediting human actions. Therefore, we propose that defining an HFE scope should include the following two considerations:

- The HFE by itself impacts plant or system status or an important component.
- The HFE involves the complete set of macrocognitive functions (i.e., detecting, understanding, deciding, and action) to achieve the HFE's objective.

Examples – *In a loss of feedwater event, feed-and-bleed is used to provide RCS cooling. It is observed that some PRA models present "feed" and "bleed" actions as two separate HFEs while others use one HFE to model both "feed" and "bleed." A similar example can be found performing the cooldown and depressurize RCS in a SGTR event.*

Analyst variations in defining HFE scope could have the following two effects:

- Most HRA methods simply use the HFEs or basic events defined in PRA models as the analysis unit applied to the HRA methods to calculate the HEPs. If an HRA method is blindly applied without evaluating the HFE scope question, the final HEPs derived from using different HRA methods could be significantly different. In the feed-and-bleed

example mentioned above, modeling the feed-and-bleed as one HFE (feed-and-bleed) versus two HFEs ("feed" and "bleed") could have a factor of two difference in HEP.

- A common HRA practice to calculate an HFE's HEP is to calculate the HFE's independent HEP first, then apply the dependency rules to modify the HEP to become a dependent HEP if there are other HFEs in the same event sequence. The joint HEP of an event sequence is the product of the dependent HEPs of all HFEs in the event sequence. In the feed-and-bleed example mentioned above, with and without considering the dependency effects could cause variation in the joint HEP.

The following guidelines emphasize incorporating human cognitive considerations into scoping the HFEs:

- An HFE should represent a complete macrocognitive process including detecting information, understanding the situation, making a response decision, and performing actions. Therefore, an HFE must include the complete cognitive process. The process starts with the stimuli (e.g., alarms, procedures) that trigger the operator's cognitive process and eventually leads to performance of the task, ending when the task is completed or the task success criteria are met. For the first HFE of an event sequence, stimuli detection starts at the initiating event. For the other HFEs, stimuli detection starts at the end of the previous HFE within the same event sequence.
  Example – *In a SGTR event, the key operator's actions are to isolate the broken SG(s) (to prevent radioactivity release) and to cooldown-and-depressurize the RCS (to stop the RCS leakage). These two actions deal with two different plant safety functions, therefore it is more convenient to model them as two HFEs. The HFE "isolate the broken SG(s)" is the first HFE of the event sequence. Its cognitive process starts at the reactor trip and ends when the broken SG(s) is isolated. Any cognitive activities in between (e.g., identify this is a SGTR event and identify that the broken SG(s)) belong within this HFE's scope. The scope of the second HFE, "cooldown and depressurize RCS," starts at the end of the previous HFE (i.e., the broken SG(s) was isolated) and ends at the completion of the RCS cooldown-and-depressurize task (i.e., the reactor is at a safe and stable state).*
- The intertwined human actions to achieve the same objective generally should be modeled as an HFE.
  Example – *The purpose of the feed-and-bleed actions in PWRs is to provide RCS cooling by iteratively feeding and bleeding the RCS. The feed and bleed actions in principal should be modeled as one HFE if the consequence is the same regardless failure of either feed or bleed.*
- If different failure modes of an HFE would result in significantly different scenarios and consequences then these failure modes should be explicitly modeled.
  Example *– Consider an overcooling event caused by stuck-open steam generator safety relief valves, normally if an analyst is just looking at core damage, the analyst doesn't particularly care about the human actions on the faulted SG as long as there is enough heat removal from the remaining steam generators (SGs). The faulted SG does not affect the core damage risk. However, if the scenario develops to core damage, the*

operator's actions in response to the faulted SG could affect level 2 PRA results. Depending on the plant's training and procedures, the operator may isolate the faulted SG from feedwater or reduce feedwater flow to maintain the faulted SG water level. In the isolation case, the faulted SG will be in a hot dry condition when core damage occurs. With high RCS pressure in level 2 PRA, the faulted SG poses a higher conditional probability of an induced tube rupture event than if secondary water level is maintained for the faulted SG. This affects the level 2 PRA's results. So if an analyst only looking at core damage in a level 1 PRA, the operators' actions regarding the faulted SG may not be identified. However, different actions to control feedwater in the faulted SG(s) affect the availability of SGs for heat removal and the availability of water in a SG to protect the SG in a level 2 PRA. Therefore, if the end consequence of interest is offsite consequence, even though performing a level 1 analysis, the analysts should include the human actions that may have latent effects on the end consequence.
***Example** - After loss of core cooling, the operator is required to manually depressurize the reactor pressure vessel (RPV). The possible error modes could be not depressurizing or overly depressurizing the RPV. The first error would result in RPV failed at high pressure. The latter results in RPV failed at low pressure because the operator fails to close the opened valve in time. Because the two failure modes have significant effects on event sequence progression from the thermal-hydraulic perspective and plant risk perspective, they may be modeled as two different top events in PRA (RPV failed at high pressure and RPV failed at low pressure). The HRA analysts should work with the PRA analysts and thermal-hydraulic analysts to incorporate the failure modes into the PRA model.*

3.1.4 Errors of commission

In the ASME/ANS PRA Standard[2], the HFEs include errors of omission (EOOs) and errors of commission (EOCs). However, explicitly modeling EOCs in PRA models is not a common practice, as stated in the PRA Procedure Guide [9]:

> However, certain types of human error are more amenable than others to exclusion in system modeling. For example, human errors associated with manufacturing are difficult to quantify, as are operator acts of commission because such a broad spectrum of actions would be candidates for evaluation.

In addition, the ASME/ANS PRA Standard [2] HLR-HR-F requirement only mentions modeling EOOs:

> Human failure events shall be defined that represent the impact of not properly performing the required responses, in a manner consistent with the structure and level of detail of the accident sequences.

NUREG-1921 provides detailed discussion of responding to spurious indications in fire scenarios. Because the discussion is relevant to EOCs, the NUREG-1921 discussion is quoted below:

An *undesired action* is defined as a well-intentioned operator action that is inappropriate for a specific context and that unintentionally aggravates the scenario. Undesired responses consist primarily of shutting down or changing the state of mitigating equipment in a way that increases the need for safe shutdown systems, structures, and components (SSCs). The key criterion in identifying undesired operator actions is that the action leads to a worsened plant state (e.g., turning a transient initiating event into a consequential LOCA). If an operator responds to a spurious indication and the action is judged not to impact the CCDP or CLERP, it does not need to be considered further.

Sources of spurious indications and alarms include degraded I&C, digital I&C failure due to software problems, and hazard events such fire. For example, spurious indications occur when electrical cables routed through a zone in which the fire is postulated are shorted, grounded, or opened as the cable insulation is burned. These instrument wires feed alarms and control indications that act as cues for operator actions. Therefore, an undesired action can be triggered through a false cue that tells the operator to take an action that is potentially detrimental to safe shutdown. For example, an action is classified as *undesirable* if the operators conclude, from false cues, that the safety injection (SI) termination criteria are met and then shut down SI when it is inappropriate to do so. In addition, if the instrument fails to operate because of damage and the cue is not provided to the operator, an action could fail to be taken (i.e., an error of omission could occur) that could also be detrimental to safe shutdown.

The undesired operator actions are identified within the context of the accident progression. When the EOPs are implemented, the operators follow them and remain in the EOP network until the plant has reached a safe, stable state, at which time normal procedures can be implemented again. During the initial EOP response, the operators are trained to respond only to indications, annunciators, or alarms that are referenced in the EOPs or that are pertinent to the scenario. In practice, when the accident diagnosis is complete, the required equipment status is verified and the plant is stabilized, the operators would resume normal protocol for monitoring the control room and attending to annunciators or alarms. In a fire scenario, the operators would also implement the fire procedures, either in parallel with the EOPs or by suspending the EOPs while the fire procedure(s) are performed, depending on plant-specific procedural guidance and training. [NUREG-1921]

This guidance suggests that HRA analysts should as a minimum identify EOCs that have the following characteristics:

- The action directly disables a safety system, sub-system or component needed to provide the plant function required in the scenario, and
- There is a rational justification to indicate that the EOC is more than a random event.

Example *- Shedding the dc load is a time critical task in an SBO event. An example plant requires the operator to open 136 breakers in 24 panels located in the cable spreading room, MCC rooms, and turbine building within 45 minutes. Because of the SBO, the normal lighting is not available, the operator has to rely on emergency lighting and flash lights to perform the task. Many of these breakers are surrounded by other the breakers with the same appearance except the labels. The operator has to compare the breakers' labels between the procedure and*

instrument to identify the correct breakers to open. While the operator's objective is to open the breakers as soon as possible to save dc power, mistakenly opening a breaker that should not be opened could happen given the number of breakers to be opened, poor lighting, and the breakers' similar appearance. This EOC could disable needed safety functions. For example, disabling the SRVs would result in the consequence that the RPV could not be depressurized. Disabling the RCIC would result in loss of RPV injection. Actions to detect and correct the EOC may delay and complicate event mitigation.

***Example -** Incorrect diagnosis leads to different actions: the PWR severe accident management guidelines (SAMGs) instruct the plant staff to use SGs to cool RCS if SGs are available. If the SGs are not available (e.g., primary system and secondary system decoupled), some plants require the RCS to be depressurized to use RWST gravity feed to RCS to cool the core. In a complex situation, the plant staff could have misdiagnosed a coupled primary system and secondary systems as decoupled or vice versa. An example can be found in the US HRA Benchmark study [NUREG-2156, draft], in the scenario with a combination of loss of feed water and SGTR, where one of the four crews did not detected the SGTR. For this crew, the SG with a tube rupture had a water level shown in the narrow range (because the SGTR flow) but the other intact SGs had narrow ranges that were off-scale low. Without diagnosing a SGTR, the crew mistakenly interpreted the high SG water level in the broken SG as an indication that they had an active loop (or a SG was available for core cooling). This misdiagnosis led to an incorrect decision that complicated the scenario.*

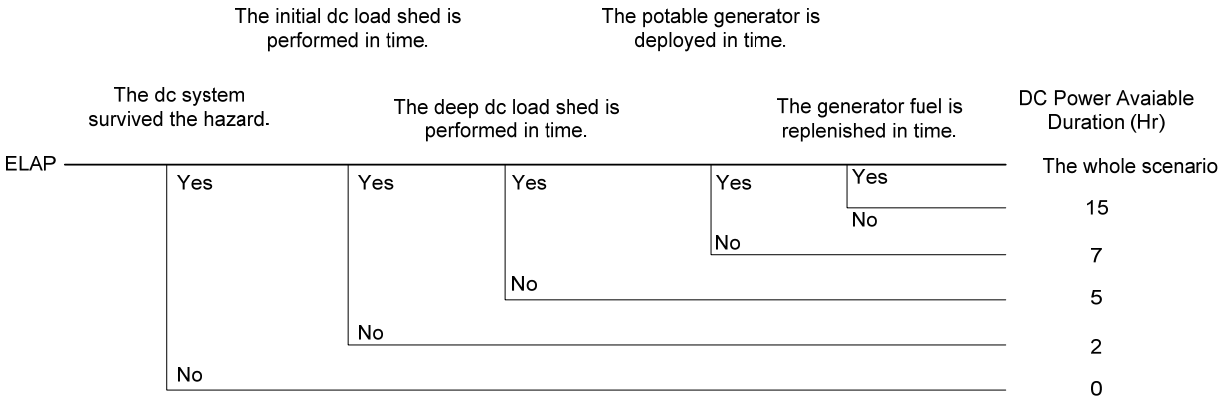
3.1.5 Define the HFEs

The PRA analysts and HRA analysts could define the HFEs differently. The analysts should work together to have consistent definitions and HFEs in the PRA model.

***Example –** In an ELAP event, shedding the dc load and using the portable generator to charge the essential batteries are important human actions. A plant applies two levels of dc load shed: (1) an initial dc load shed after an SBO is declared; and (2) a deep dc load shed after an ELAP is declared. Human failures in not shedding dc load could have the following variations (Table 2):*

- *The initial dc load shed is not performed: The essential dc batteries will deplete within 2 hours.*
- *The initial dc load shed is successfully performed: The essential dc batteries will deplete within 5 hours.*
- *Both the initial dc load shed and the deep dc load shed are successfully performed: The essential dc batteries will deplete within 7 hours.*
- *The portable diesel generator is successfully used to charge the essential batteries but without fuel replenish: The essential batteries operation time is extended for additional 12 hours.*
- *The portable diesel generator is successfully used to charge the essential batteries with fuel replenish: The essential batteries operate throughout the whole scenario.*

The PRA analyst may want to combine these variations in the PRA model to reduce the event tree size. For example, using two HFEs, instead of five HFEs, to model the above five variations. The HRA analyst should work with the PRA analysts to identify optimal modeling and definitions of the event tree top events.



Note: The time information in the above tree is only to illustrate human actions' effects. The values do not represent any plant.

Table 3-1 Example of dc availability in an ELAP event related to human error in shedding the dc load and charging the essential dc batteries with a portable generator.

HFEs are typically defined in conjunction with HFE identification and, as the PRA develops, the definition is refined and revised. The ASME/ANS PRA Standard HLR-HR-F outlines the requirements for definition as the following: "Human failure events shall be defined that represent the impact of not properly performing the required responses, in a manner consistent with the structure and level of detail of the accident sequences." Consistent with these requirements, the definition activities described in this section are those associated with understanding the PRA boundary conditions for the HFE and the tasks involved in crediting plant staff actions in the PRA.

For the identified HFEs, the response failures should be defined to represent the impact of the human failures at the function, system, train, or component level as appropriate. The definition should start with the collection of information from PRA and engineering analyses, such as the following:

- Accident sequences, the initiating event, and subsequent system and operator action successes and failures preceding the HFE
- Accident sequence-specific procedural guidance
- The cues and other indications for detection and evaluation of errors
- Accident sequence-specific timing of cues and the time available for successful completion
- The time available for action
- The high-level tasks required to achieve the goal of the response

Once this information is gathered, the HFE can be defined at the level describing the human failure of not performing or not properly performing the required actions. This specifies the component, train, system, or plant function affected by the actions. The definition should include the effects of the human failure in the scenario.

3.2 HFE feasibility assessment

Once the operator action has been identified and the HFE defined, the HRA analyst should initially determine if the operator action is feasible in the event context. The purpose of the feasibility check is to ensure that the PRA is not crediting an infeasible operator action. At this stage in the HFE development, the initial feasibility assessment is primarily conducted based on information obtained from scenario analysis supplemented by any additional information that

may be known about the particular action or PRA scenario. Feasibility should be treated like a "continuous action step" and reviewed periodically as the HFE is further developed and refined. This initial assessment is intended to screen out those operator actions that are obviously not feasible. At this stage, any EOP-based actions should be considered feasible and should be carried forward in the analysis.

If an operator action is not feasible, then the HEP should be set to 1.0, or the HFE need not be included in the PRA logic model. After the preliminary results have been incorporated into the model, additional resources can be used to reassess actions that were previously considered not feasible. There will always be cases in which, with enough information, the HRA analyst could make an argument that an action is feasible even though the initial information suggests that the action will be extremely difficult or vice versa.

3.2.1 Feasibility Assessment Criteria

This section provides guidance for an initial assessment of feasibility during the Identification and Definition phase of the HRA analysis to decide whether an HFE should be included in the model. For example, a response will not be feasible if the equipment required to perform the response is not available, or the indications needed to alert the operators to the condition(s) requiring a response are not available. The assessment performed during this early phase of the analysis is essentially a check to avoid including any action that is obviously not feasible and does not require a detailed timing analysis. However, a more detailed assessment will be needed as the necessary contextual and timing information are obtained.

The questions presented below present feasibility considerations. Any of the following six feasibility considerations does not meet the feasibility screening criteria and should result in infeasible actions.

- **Sufficient time:** This is by assuming that everything goes as planned without surprise, performing the action requires more time than what is available. An example is the Monticello Nuclear Generating Plant SDP analysis [ML13240A435] where the HFE is to construct a long levee including the procurement of the construction materials within a specified time.
- **Credible cue(s):** There must be credible cue(s) (or information) to lead the operator to be aware of the need to perform the HFE.
- **Procedures and training:** The feasibility analysis should include evaluation of the availability of procedures and training to perform the HFE of analysis.
- **Sufficient manpower and skills:** Having sufficient manpower and all needed skills (or abilities) to perform the HFE.
- **Accessibility:** The action location and the travel route to the action location must be accessible.
- **Equipment and resources:** The needed component, equipment, parts, and vehicle, etc., are available to complete the HFE.

These six criteria are consistent with the following six considerations in [EPRI 1025294] for performing a feasibility check:

- Time
- Cues
- Procedures and Training
- Manpower
- Accessible Location and Environmental Factors

- Equipment Accessibility, Availability and Operability

The only difference from the IDHEAS-G approach is in the manpower item. The IDHEAS-G methodology requires a combination of sufficient manpower and the needed skills (or abilities) to perform the task. For example, in an extreme external hazard the plant security force may be required to support the trained plant staff to remove the debris on the road and move the portable equipment to the equipment staging location. These activities require more than one person. But everyone on the team does not need to have specific skills. In most instances, other plant staff without the specific skills (e.g., security and chemistry) can supplement the manpower needed if they are under supervision of plant staff with the specific skills and knowledge. The combination of staffing and skills make the task feasible.

The EPRI 1025294 guidance indicates that the above six considerations are not necessarily complete. Some unique contexts may present additional considerations when determining feasibility. The EPRI 1025294 guidance states, "However, this list is meant to be an initial checklist and is not meant to be all encompassing. If there are additional contextual factors or performance shaping factors not explicitly listed that would lead to failure of the operators to achieve the modeled success criteria, then the associated HEP should be set to 1.0 as the operator action would not be feasible." Similarly, the six criteria proposed above for the IDHEAS-G methodology are only for the initial feasibility check. The HRA analysts would need to identify if there are unique consideration to determine feasibility for their analyses.

NUREG-1921 [4] adapted various feasibility criteria to the fire HRA domain and provided further guidance on determining whether the criteria are met. In comparison to EPRI 1025294, NUREG-1921 has one additional criterion (i.e., the relevant components are operable) in assessing feasibility. The following are the seven feasibility criteria considered in NUREG-1921:

- Sufficient Time
- Primary Cues Available/Sufficient
- Proceduralized and Trained Actions
- Sufficient Manpower
- Accessible Location
- Equipment and Tools Available and Accessible
- Relevant Components Are Operable

The "relevant components are operable" criterion is to be assessed by PRA analysts rather than HRA analysts. IDHEAS-G has included this consideration in the "Equipment Accessibility, Availability and Operability" criterion.

Thus, the IDHEAS-G criteria for performing an initial feasibility check are consistent with the criteria used in other HRA approaches.

3.3 Feasibility Assessment Guidance

This section presents guidance to assess each feasibility assessment factor. Failure to meet any one of these criteria leads to the determination that an HFE is not feasible (i.e., the HEP is 1.0), meaning that the operator response cannot be credited in the PRA.

3.3.1 Sufficient Time

Sufficient time in feasibility assessment means that the required human actions can be successfully performed at a normal pace and without complications within the time window during which the actions must be performed to avoid adverse consequences, as defined by the scenario. That is, there is sufficient time for human actions if the time required to successfully perform the HFE is less than the time available for the HFE. The time required is a sum of the following three time periods:

- Delay time: This is the amount of time that elapses between the point in time at which the plant abnormality occurs and the point in time at which cues about the abnormality become available to the operators.
- Diagnosis time: This is the amount of time that elapses between the point in time at which cues become available to the operators and the point in time at which the operators decide on a response. For control room actions, this typically is the time spent on implementing information-gathering steps in the applicable procedure up to the point in time at which the first mitigation action step in the procedure is performed. For human actions that are not governed by an applicable procedure, the plant staff would need to develop a response plan. The HRA analysts would have to estimate the time that would be taken to have the response plan in place.
- Action time: This is the time that elapses between the point in time at which the response plan is implemented and the point in time at which the action is completed. For simple actions inside the MCR, action times are typically less than one minute. For local actions, the action time could include travel time to the work or equipment location, moving the equipment to its staging location, setting up the equipment, and performing the actions. If the actions require special materials or equipment that are not readily available on site, the time required for procurement and transportation, etc. has to be included in the action time.

3.3.2 Credible Cues

Cues of interest in a feasibility assessment include the initial signal or plant symptom that becomes available to operators to make them aware of the plant abnormality (or the need to perform an HFE) and the related information to solve the problem. A cue could be present for detection, for example, via plant instrumentation, alarms, a plant walkdown, or credible engineering judgments. It is assumed that without the initial cue(s) to hint about the plant abnormality the operator will not respond to the abnormal situation. In most cases, the cue(s) are presented by instrumentation and alarms. The MCR of a NPP is equipped with about 1,000 alarms and many indicators to provide cues for operators to respond to a wide range of plant abnormalities. The advanced digital instrumentation and control MCR has more indications and alarms to provide more specific information to the plant operators than a conventional MCR.

When performing a feasibility assessment on cue availability, the analysts should view the cue(s) from the operators' perspective to identify credible cues. These are cues that are more likely to catch the operators' attention, instead of all of the cues that may be present or listed in procedures. In addition, there are often redundant cues pointing to a plant abnormality. These redundant cues should also be considered to be credible.

Plant walkdowns, as required by procedures, and information exchanged during shift turnovers may also support operators' detection of plant abnormality symptoms that may not be detected in the MCR. The HRA analysts should evaluate the conditions that are covered by a plant walkdown and the plant walkdown route that would be taken in order to identify the credible cues.

Credible engineering judgments may include cues such as a loud noise from a main steam line PORV actuation that is clearly audible to the MCR crew or plant status information derived from plant engineering knowledge. For example, in the Fukushima Daiichi event, all instrumentation and alarms were lost after the loss of both ac and dc power. Under such a situation, the operators had a mental model from training that helped them to estimate plant status (e.g., the time to reach core uncovery) in the near future to guide their actions. Overall, operators are expected to pay attention to the following major safety functions [NUREG-1122 and NUREG-1123]:

1. Reactivity Control
2. Reactor Water Inventory Control
3. Reactor Pressure Control
4. Heat Removal From the Core
5. Containment Integrity
6. Electrical
7. Instrumentation
8. Plant Service Systems
9. Radioactivity Release

In addition, the operators would protect the site from external hazards if advance warning and preparation time is available (e.g., a flood event). Most of the above items are listed in operating procedures. The point is that the operators maintain a general awareness of the indications related to the safety functions statuses.

3.3.3 Procedures and Training

The ASME/ANS PRA Standard [6] Supporting Requirement HR-H2 states that human recovery actions can be credited if "a procedure is available and operator training has included the action as part of crew's training, or justification for the omission for one or both is provided." The cues discussed in the previous section trigger operators to attend to the plant abnormality and motivate the operators to look for additional information that would eventually lead to the HFE actions. In most cases, procedures and training should be available for the operators to successfully implement the HFE.

In certain situations, proceduralized mitigation strategies may not be applicable to the specific situation. This is likely to occur in ASP and SDP analyses but unlikely in the basic PRA. For example, the procedure-instructed system alignments may not work for an event with multiple latent failures. But a feasible system alignment can be identified with engineering judgment to achieve the same plant function. Even though the alternative option is not explicitly listed in the procedures, the option may be credited in an HRA if sufficient time is available for identifying the alternative alignment and to implement the actions.

3.3.4 Sufficient Staffing and Skills

Feasibility assessment of staffing includes an evaluation of the availability of a sufficient number of trained personnel without collateral duties for an HFE, such that the required operator actions can be completed as needed. If there are not enough crew members available to complete all of the tasks that must be performed within the same time interval (i.e., the number of people required for each task exceeds the number of crew available), the HEP should be set to 1.0.

Staffing issues such as the following should be considered in the feasibility assessment:

- Some MCR personnel may not be available for a period of time after an initiating event (e.g., the shift manager is normally in an office near the main control room but not in the main control room. The shift manager and the shift technical advisor in the H.B. Robinson fire event was in a different building for shift turnover).
- Consideration should be given to the workload of the MCR crew while responding to the event, particularly if it appears to be a relatively cognitively challenging scenario or requires a complex response such as directing and coordinating multiple teams involved in executing the actions, particularly if the MCR crew has other significant responsibilities at the same time. Workload issues are also discussed further below.
- If onsite or offsite personnel have to be summoned, an assessment of how long it will take them to get to the control room or the site should be performed, considering the likely starting locations for the personnel. The analysis should consider the potential that the personnel might be in remote locations from which it may be difficult to egress and that the personnel may have to complete some actions before they can leave an area. If the actions will involve multiple staff in certain sequences, these activities, their coordination, and their associated communication aspects should be assessed.
- For an extreme event blocking site accessibility for a certain period of time, the tasks to be performed have to rely on the onsite personnel before the offsite personnel are available. It would be necessary to perform a staffing analysis to ensure that sufficient personnel and needed skills are available for all essential tasks.

3.3.5 Accessible Location

For actions outside the MCR, if it is known that the operators will not be able to reach to the location(s) to perform the required critical tasks, the operator actions should not be considered feasible.

The evaluation of “accessibility” mandates an evaluation of the travel path required for local actions and how such accessibility might be compromised in the event. It may be necessary to postulate alternative actions that can be taken in other locations to achieve the same goal or function, as long as these alternative actions are verified as feasible through operator interviews and plant walkdowns. Travel routes should be identified and documented using the plant layout diagrams (indicating the specific room, stairwell, and doorway numbers) and verified with operations staff to ensure correctness for the given scenario. Analysts should consider including radiation hotspots and radiation areas as an additional, potential information source in discussing possible impact on travel paths. The impact of alternative travel paths on the HFE execution timing should also be considered because, for short timeframe actions, the addition of further travel time could render the action infeasible.

Environmental and other effects that might exist in an event scenario include the following:

- Steam or water on the floor from the occurrence of the initiating event
- Fire and related smoke, heat, and toxic gas effects.
- Obstruction, such as from charged fire hoses or equipment present during shutdown activities.
- Radiation. For the feasibility analysis, the analyst needs to determine whether the radiation level or rating of an area would preclude access or otherwise prevent the action from being feasible.
- Locked doors. An event initiator such as fire or flood may cause electric security systems to fail locked. In this case, the operators will need to obtain keys for access. If all operators do not routinely carry the keys to access a secure area, the analyst must ensure that there is enough time for the operators to obtain access. Normally locked doors should also be considered. At some plants, the security system may be adversely affected by the loss of the preferred or Class 1E power supplies. In such cases, some manual actions may require additional actions to obtain access to the Protected Area and internal locked areas where remote equipment operation is necessary.
- Road block. If portable equipment is used, vehicles may be used to transport the equipment. The transportation routes may be blocked by the damaged structures and debris resulted from the hazard.

3.3.6 Equipment and resources

To manipulate plant equipment locally, portable and special equipment, tools, special parts, and vehicles, etc. may be needed. Their feasibilities should be considered. The equipment discussed here includes all things needed to support the equipment operation. For example, for a portable diesel pump, the equipment could include the vehicle to tow the pump to its staging location, the water source (e.g., fire hydrant or ultimate heat sink), pipes, hoses, junctions and fitting, etc. to withdraw the water source and to deliver the water to the desired location, and the fuel to run the pump. According to NUREG-1852 [5] items such as keys to open locked areas (especially in light of tighter key controls that some plants may have implemented in response to security needs) or allow manipulation of locked controls, portable radios, portable generators, torque devices to turn handwheels or open flanges, flashlights, ladders to reach high places, and electrical breaker rack-out tools.

Training on the use of this equipment is important to crediting feasibility, and the training quality and frequency should be noted during the feasibility assessment.

3.4 Screening Assessment

In the IDHEAS-G process, the identified HFEs are assessed for their feasibility, and the feasible HFEs are to be further analyzed and quantified. In reality, PRA practices typically perform a screening analysis for feasible HFEs before diving into the detailed analysis. These three types of analysis serve different purposes in PRA practices:

3.4.1 Feasibility analysis –

The analysis is to determine if an HFE is feasible to be performed in the context of the analyzed event by applying a small set of criteria. The assessment outcome is binary: not feasible (HEP = 1.0) and feasible (HEP ≠ 1.0). A HFE is determined as feasible does not mean that the HFE is reliable. An infeasible HFE could result in changes in the PRA model (not able to credit the HFE or replace the HFE with a feasible approach), procedure change, and changes to plant design (e.g., install new detection instrument), etc. The feasibility assessment is conducted in the early stage of a project to have a stable event tree structure.

Example - *Monticello Nuclear Generating Plant SDP analysis [ML13240A435] can be seen as a feasibility assessment. The HFE of interest was to prepare for an extreme flood by building levee and bin wall system within 12 days (the time frame stated in the licensing basis). The levee to be constructed include a 2080 feet of earthen levee and 320 feet of bin walls. The SDP analysis concluded that the time to procure the construction material and to install the bin wall will significantly exceed the 12 days available time. Therefore, the HFE of building a levee to protect the plant facility was not feasible and wan not credited in this SDP analysis.*

3.4.2 Screening analysis

This analysis is to provide quick HEPs for the PRA project to move forward. In a multiple disciplines PRA project, the thermal-hydraulic analysts need to prioritize simulation sequence based on the PRA event tree. HEPs are needed in the event tree to determine the event sequence priority. At this time, the HRA analysts are likely not having the detail analysis performed so the screening or scoping assessments provide quick HEP values to support the project needs. They may be replaced by the detail HEPs in the later phase of the PRA project. The quick HEPs typically refer to the HEPs generated based on simple rules. For example, as a common practice, the HEPs of 0.1 and 0.3 are used for MCR and ex-MCR action in the level-1 internal event PRA. These HEPs are expected to be conservative.

3.4.3 Detailed analysis

The analysis is to provide detailed qualitative and quantitative information about the HFE. The qualitative information includes the expected crew responses and critical tasks involved, potential recovery paths for failing the responses, the detailed timeline of the responses, and time uncertainties. The quantification information includes crew failure modes in the HFE, the PIFs affecting the HFE, and estimation of the HEP.

Additional information on screening analysis -

For fire HRA, NUREG-1921 improved NUREG/CR-6850's screening instruction by classifying human actions into short term actions (the actions to be performed within one hour of the fire event) and long term action (the action does not need to be performed within one hour after the fire event initiation). Four screen HEP values are used in the NUREG-1921 including:

- *Same as the internal event HEP of the HFE*
- *10 times of the internal event HEP of the HFE*
- *0.1*
- *1.0*

The following table is provided in NUREG-1921 to summarize the screen rules.

Screening Criteria	**Short-Term Human Action**		**Long-Term Human Action**	
	Definition	**Value**	**Definition**	**Value**
Set 1: similar to internal events HFE but with some fire effects	Required within first hour of fire/trip	10x internal events HEP	Performed ~1 hour after fire/trip (fire effects no longer dynamic, equipment damage understood, and fire does not significantly affect ability of operators to perform action)	Same as internal events HEP
Set 2: similar to Set 1 but with spurious equipment or instrumentation effects in one safety-related train/division.		0.1, or 10x internal events HEPs, whichever is greater		0.1, or 10x internal events HEP, whichever is smaller
Set 3: new fire HFEs or prior internal events HFEs needing to be significantly		1.0		0.1, or 10x internal events HEP,

modified as a result of fire conditions				whichever is smaller
Set 4: alternate shutdown (including MCR abandonment)	1.0 for initial screening or 0.1 following qualitative analysis			

4 HFE qualitative analysis – Task analysis & time uncertainty analysis

The purpose of this step is to perform and document a task analysis of the overall responses to identify opportunities for the plant operators to make errors within a HFE. Identification of these opportunities requires an identification and definition of the critical tasks in the performance of the response. In the following, a critical task is identified with the significant transition points in the response, such as entering a procedure, transitioning to another procedure, deciding how to respond to the situation, and execution. Success in performing a critical task may require the successful performance of one or more specific cognitive and execution activities such as collecting data, and comparing data to a decision criterion. Failure to perform any of the critical tasks results in the HFE. In addition, because there may be opportunities for the operating crew to recover from an error within the time window, the task analysis also identifies opportunities for such error recoveries.

The crew response diagram (CRD) is to communicate, illustrate, and document the outcomes of the task analysis. The opportunities for both errors and for error recovery are represented as nodes on the CRD. In parallel, as an essential part of developing the CRD, a detail timeline may be developed to facilitate understanding of the details. The CRD timeline is more detail than the timeline of the baseline scenario. The subject of the CRD timeline is an HFE while the subject of the baseline scenario timeline is the whole scenario. The CRD timeline identifies the specific actions and error recovery opportunities only related to the HFE of analysis. The baseline scenario timeline include all HFEs and hardware responses occurred in the scenario that their success and failure will change the course of scenario progression. The CRD timeline captures:

- the plant status trajectory in terms of the timing of cues and other plant process parameters that are required trigger the crew to respond to the situation, to perform the right actions, and to realize an opportunity for error recovery
- the time at which operators are expected to reach critical steps in the procedure or the critical actions are performed.

If, at any stage in the development of the task analysis, it can be determined that based on the more detailed information obtained in the task analysis and CRD timeline, the HFE can be determined as not feasible (based on the criteria addressed in the HFE feasibility analysis such as sufficient staffing and time) then the HFE's HEP is set to 1 and the HFE analysis is terminated. For example, the CRD timeline may reveal that the time needed by the operators to follow through the procedure to reach to the action point is too long for the response to be successful.

4.1 Background information – Task analysis and cognitive tasks in NPP

4.1.1 Task Definition

One traditional question in performing an HRA is the level of details of breaking an HFE into tasks. A HFE can be broken into tasks at any arbitrary level of granularity; In the IDHEAS framework, a HFE should be broken into tasks at a level that retains the HFE context and directly links to cognitive functions. There are no absolute criteria for the level of tasks in IDHEAS. Below is some general guidance on identifying a task:

- What is a task:
  - A task constitutes a recognizable and consequential unit of human activities;
  - A task needs to be made by human to achieve a desired plant status;
  - A task includes all four cognitive functions (detecting, understanding, deciding, and actions);
  - Successfully perform the action portion of the task will alter the scenario course toward safer plant status
- Boundaries between tasks can be distinguished by any of the following:
  - Clearly defined goal
  - Clearly defined initial or entry state
  - Clearly defined ending or exit state (i.e., consequences or outputs)

4.1.2 Macro-cognitive functions and activities

This sections explains the four macro-cognitive functions (*detection, understanding, decision-making, and action execution*) and provides examples of the activities of these macro-cognitive functions. The phrase 'macrocognitive' is intended to highlight that individual and team cognition is modeled at a 'macro' *functional level* of description. The team-related effects on human performance such as communication, coordination, supervision, and error recovery, etc. are considered in assessing the challenges in performing the macrocognitive functions.

4.1.2.1 Detection

Detection is to obtain meaningful information pertinent to the task goal. The following are some cognitive activities of detection:

- Attending to alerts or alarms – Urgent information that requires operators' immediate attention are presented saliently so that they can pop out of scenes and attract operators' attention

- Check or collect information (i.e., goal-directed information acquiring) - The information is displayed in the means such as indications, computer displays, manuscript, and drawings, etc. Operators get information from a known source or searched through the working place.

- Monitor system parameters or status – Monitoring is a continuous or intermitted detection activity to check or verify if some parameters or system status are expected or abnormal.

Information can be directly perceived through human sense organs (e.g., visually seeing the water level of a pool, hearing a loud roar of main steam safety valves opening, touching a pipe to feel the vibration to determine if there is water flow, sensing the ground vibration in a seismic event) or it can be measured or detected with use of an equipment (e.g., area temperature can be obtained with use of a thermography gun). As the information is perceived through the sensory organ or equipment, operators needs to recognize the meaning of the perception and mentally or physically categorize the information.

Additional information:

Detection in NPP control rooms

The typical cues related to plant safety are alarms and indicators. There are situations when other types of cue are available such as noise (e.g., the loud steam release noise from steam relief valves), on-site reports (e.g., fires and large chemical spills that affect the control room ventilation system), off-site reports (e.g., tornados and electric network load changes), and others (e.g., automatic system actuations and vibrations due to earthquakes). A typical control room has about 1000 alarms, a large number of control panel indicators, and computer displays to indicate a wide range of plant, system, and component status for plant operations and safety. Status changes to any of the alarm, indicators, computer displays could serve as a cue to indicate a plant malfunction exists. It is unperceivable that a plant malfunction threatening plant safety is not indicated by these indications. In fact, in PRA context, a plant malfunction would typically change the status of multiple indications to cue the operators that there is something wrong with the plant.

Operating experience shows that the operators typically do a good job in detecting cues. The situations in which the cues may be not detected in time are typically associated with multiple plant malfunctions occurring simultaneously. For instance, the operators are paying full attention to dealing with one malfunction and do not detect the cues of another malfunction; latent failures occur with concurrent plat malfunctions; long durations exist between the cue and the needed actions so that the cue was forgotten (no action was performed); and fatigue (an issue more related to plant security instead of safety).

4.1.2.2 Understanding

The understanding function is to integrate multiple pieces of information to obtain a piece of information that none of these single indications can directly indicate. The following are some typical cognitive activities of Understanding:

- Maintaining situational awareness based on directly available information – In becoming aware of the system status such as the occurrence of a steam generator tube rupture, there is no single indication for the status. It has to be determined based on evaluation of multiple pieces of information such as main steam line radiation, SG water level, and the blow down line radiation, etc. Operators form the situational awareness of the system status by integrating information from the indications.
- Assessing system status based on non-direct information - Assessing system status typically involves integration, process, and inference of many pieces of information to come up with an interpretation of the information. For example, assessment of a NPP core damage involves many aspects of the plant status such as whether core debris has relocated, whether the RPV is breached, and whether the containment has an uncontrolled breach, etc. These plant statuses do not have indicators directly revealing their statuses; the crew has to integrate multiple pieces of information to reach to a conclusion.
- Diagnosing problems and resolving conflicts in information - to understand the causes of abnormal signals or conflicts in data requires reasoning. For example, a pump or turbine vibration is what actuated trouble alarms of multiple components at different locations (e.g., a instrumentation air leak event or an electric problem that affect multiple components), or identifying the radioactivity

release need to understand the path from the reactor vessel to containment then to outside environment in severe accidents.
- Predicting trends or event evolution

Understanding is based on information detection. In some situations, the operator may do something (e.g., open and reclose a pressurizer PORV verify if the valve is leaking that caused the observed RCS pressure decrease) in order to obtain information for diagnosis. The purpose of the action is part of diagnosis process to gather additional information to understand the plant status. Therefore, the action is part of the understanding function. The distinction between Detection and Understanding functions is that Detection is about individual pieces of information while Understanding involves integrating multiple pieces of information with one's mental model of the object being understood. In the future DI&C control rooms, the DI&C may automatically gather the specific plant parameters' statuses and automatically assess the plant status, integrate the information, performing reasoning, and present a direct indication of the plant status to the plant personnel. Thereby, many activities involving Understanding may become Detection only.

Additional information - Understanding in NPP control room operation

Diagnosis activities occur after the Detection macrocognitive function and before the Decision-making /Response-planning macrocognitive function, yet these functions are performed iteratively until the objectives are achieved. After a plant abnormality cue is detected, the operators are trained to (and typically would) verify the cue by immediately checking indications related to the cue and diagnosing and understanding the plant status by checking additional plant information. The cognitive process after the cue detection belongs to the Understanding macrocognitive function. For NPP internal events, the diagnosis results would determine the response planning because the operators' emergency responses are most likely driven by procedures. Depending on the scope of the task of analysis, the boundary between diagnosis and response planning could have different level of details. For example, under an emergency condition (e.g., reactor trip) of a PWR plant, the E-0 post reactor trip response procedure is a diagnosis procedure that guides the operators toward understanding the plant status and identifying the abnormality. E-0 should eventually lead the operators to event based procedures (e.g., E-1 LOCA, E-2 MSLB, and E-3 SGTR) to handle the specific problem. Therefore, a high level classification would be the operator activities within E-0 belonging to the diagnosis macrocognitive function. The junction between diagnosis and response planning is the decision (e.g., transfer to E-3 in a SGTR event). In this case, E-3 is the response planning. However, even within the event-based procedures there are diagnosis activities. For example, identifying the broken steam generator(s) within E-3 is a diagnosis activity. The required follow on activities (i.e., isolate the broken SG(s) and corresponding preparation activities if any) belong to response planning.

In the NPP PRA context, the operators' responses to plant malfunctions are most likely guided by procedures. Before a reactor trip, the alarm response procedures (ARP) and abnormal operation procedures (AOP) are the typical procedures that guide the operators' responses. After a reactor trip, the emergency response procedures (EOP) would guide the operators' responses. The expectation is that all the design basis events will be mitigated by implementing

the EOPs. In the events that exceed the plant's design basis, the severe accident mitigation guidelines (SAMGs), the extreme damage mitigation guidelines (EDMGs), and the severe accident contingency guidelines are available for event mitigation. In addition, specific event based procedures such as earthquake procedures, fire procedures, flood procedures, etc. are available when the situations apply.

In general, the goals of the ARPs, AOPs, and EOPs are to protect the integrity of reactor fuel, fuel cladding, and reactor vessel to prevent radioactive release. In practice, the procedures guide the operators to identify the causes of plant malfunctions under the condition that sufficient plant safety margin is maintained. For example, the E-3 procedure guides the operators to identify and isolate the ruptured SG(s) to properly depressurize and cooldown the RCS and prevent radioactive release to the containment or environment. The goal of the severe accident guidelines is to prevent and mitigate radioactive release from the containment. Mitigating event consequence has a higher priority than identifying the causes of the severe event. In practice, the severe accident guidelines provide a set of mitigation strategies for the decision makers (i.e., operators or plant managers) to chose the optimal option based on the situation. This provides flexibility for the responders to decide the most optimal strategy to implement based on the situation. In some situations the plant malfunction may not meet the entry condition of any procedure. In this case the operators would need to diagnose the situation based on their knowledge. For example, instrumentation air leakage could complicate components responses such that the symptoms shown in the plant indications may not match any procedure's entry conditions. Inappropriately handling the situation could cause the failure of certain components that in turn would initiate a PRA initiating event and become a safety concern.

Diagnosis could be complicated due to various reasons such as instrumentation latent failures that provide false plant status information; inconsistency between procedure instructions and scenario progression; unfamiliarity with the specific events; masking effects on plant symptoms due to reasons such as simultaneously multiple failures; and sense of urgency in interfering with the event progression that results in prematurely concluding a diagnosis. Not all situations have corresponding procedures. In such situations, the decision makers would need to base decisions on the available information while considering information reliability and uncertainty and other factors to conclude a diagnosis for optimal response planning. During a severe event, the plant status changes may affect the optimal response planning such that the diagnosis of the plant status is a constant effort. For example, during a severe accident situation (i.e., core melt occurs) injecting water into the reactor vessel could be an optimal decision when hydrogen explosion is not a concern. But if the event progresses to potential hydrogen explosion, injecting water into the melted core may not be an optimal decision. The decision makers need to consistently diagnose plant status and change response planning as necessary.

4.1.2.3 Decision-making

Decision-making is to determine the optimal response strategy or plan to the situation among the alternatives. This includes deciding such as whether actions should be performed to respond to the situation (e.g., deciding whether to inject into RCS in a situation that hydrogen burn or deflagration is a concern), deciding how the actions should be performed, e.g., delay implementation until reaching to certain condition, and

deciding an option which is not pre-planned to best address all considerations challenging plant safety for a specific situation, etc.. The following are some examples of decision-making:

- Procedure based decisions: For nuclear power plants, this refers to the decisions in the AOPs and EOPs. Within these procedures, the major decisions had been thought through and incorporated into the procedures. The procedures made the decisions for the operators. The procedures provide detail instruction on which parameters to check (detecting), what is the problem (understanding), how to handle the problem (decision), and what specific actions to be performed (action). For example, after a reactor trip, the E-0 is entered. The E-0 guides the operator to diagnose the event based on event symptoms. After identified the problem, the procedures transfer to the corresponding event procedures (e.g., LOCA, MSLB, and SGTR) to handle the problem. The decisions are integrated into the procedures to bring the plant to safety.
- Go/No-Go decision: This is a decision on whether a task should be performed. The Westinghouse plants' severe accident guidance (SAGs) provides examples of this type of decision. Once a SAG is entered (e.g., injection into RCS), the decision maker(s) have options to implement and not to implement decision based on other plant status (e.g., hydrogen concentration). The decision output may not be simply do or not-do but also include "do it later" or "do something else first before doing it" or "do it in a specific way," e.g., to inject water into core debris with hydrogen detonation consideration, the SAG instructs to inject with small flow rate first then gradually increase the flow rate instead of a large flow rate at the beginning.
- Optimization: When the same source is needed for different tasks and these activities have similar levels of importance, the decision makers would need to decide how to balance the needs in sharing the limited resources. For example, injecting into RCS and performing containment spray could use the same water source in a situation that RCS integrity and containment integrity are challenged. To achieve the objectives of cooling the core and depressurizing containment, the decision maker(s) would need to adjust the RCS injection and containment spray based on scenario dynamics.
- Action planning - deciding on what, how and when the actions should be performed: In a sever accident situation, restoring the failed components or water source is expected to be an important task. If the restored option provides more benefits than the current option is use, a decision is when and how the restored option should be implemented to replace the current (less optimal) option. A similar decision is on the degraded component. For example, in an ELAP and LOUH event as specified in EA-12-049 and NEI 12-06, the RCIC in the choice option to inject into RPV for a BWR. If the ac power is not restored in time, the high tours temperature would fail the RCIC. The portable diesel pump is an alternative option to inject water into RPV. The RCIC has the benefits of using clean water for RPV injection. Because the portable pump has low pump head, switching from RCIC to the portable pump may require to depressurize the RPV to the point that there is no sufficient steam to drive the RCIC pump. Once the decision is made, the operator risk to have only one RCS injection option (the portable pump) instead of two. This is a drawback from the redundancy for safety consideration.
- Restoration equipment: Equipment restoration is very important during extreme events and severe accidents. The decision on the priority of equipment to be

restored depends on many factors such as the equipment restorability, urgency of needing the equipment, and man-power availability, etc.

Additional information: Decision-making in NPPs

In general, decision-making in NPPs involves operators using their situation model to identify goal states and the transformations required to achieve them. The goal state may vary, such as identifying the proper procedure, assessing the status of back-up systems, or diagnosing a problem. To meet their goals, operators generate alternative response plans, evaluate them, and select the one most appropriate to the current situation model. Response planning can be as simple as selecting an alarm response or it may involve developing a detailed plan when existing procedures proved incomplete or ineffective.

- *In an NPP, procedures usually aid response planning. The need to generate a response plan in real time largely may be eliminated when operators trust that the procedures are suitable to meet the current problem. However, even with good procedures, operators will undertake some aspects of response planning. For example, they still need to (1) identify goals based on their own situation assessment, (2) select the appropriate procedure(s), (3) evaluate whether the procedure-defined actions are sufficient to achieve those goals, and (4) adapt the procedure to the situation, if necessary.*
- *After a diagnosis process leads to an understanding of the plant, a decision to intervene upon the scenario course to ensure plant safety or to mitigate consequences based on understanding is a natural result. In NPP, the response planning includes the decision and the operators' plan to execute the decision. Use a SGTR event as an example. At a high level, the diagnosis process is represented by E-0 that guides the operators to conclude that a SGTR is the plant status. In this case, if the operator follows E-0, the operator will make a decision to use E-3 to handle the event. E-3 is the operator's response planning to respond to the SGTR event. The action (i.e., the next macrocognitive function) is to perform the activities specified in E-3. Therefore, the macrocognitive functions of response planning and action are performed simultaneously. The differences are that the response planning is about the brain (i.e., cognitive) activities, and the action is about the physical activities in interacting with the human-system interface. The response planning includes the preparation work (e.g., verifying the plant is in a correct configuration) before conducting the key actions addressing the perceived plant problem and the actions required after the key actions to very that proper actions are performed to reset the plant to a desired configuration.*

4.1.2.4 Action execution

Action execution is to perform the decided action plans to achieve a goal. For example, the SGTR emergency operating procedure (EOP) provides an explicit step-by-step action instruction to handle a SGTR. The EOP is entered because the crew concludes that a SGTR event is in progress and the crew is trained to use the SGTR procedure to handle the situation. Therefore, following the SGTR procedure involves the Action execution function.

Below are some examples of action execution:

- Following a step-by-step procedure or diagram
- Performing a procedure attachment
- Implementing an action script
- Implementing manipulations based on high-level instructions or guidance,
- Performing skill-of-craft actions.

Action execution includes receiving the action commands, confirming, clarifying, and questioning the action commands, obtaining needed access keys, tool, and equipment, traveling to the action locations, verifying the target of action (e.g., verifying component identification), executing the actions, verifying the action completion, monitoring the action effectiveness, and reporting back the completion of action. Typical actions involve the entire process of achieve the goal. Notice that a typical action process involves verifying action status and monitoring action effectiveness; these activities belong to the action execution function rather than the Detection function.

Additional information: Action execution in NPP control rooms

Actions inside the main control room are typically not challenging. Most of them include pushing a button or turning a switch. In some cases, monitoring and control type actions are required (e.g., cooldown of the RCS not exceeding 100 ºF/hr). Every action the operators are trained and required to perform follow the Stop, Think, Act, and Review (STAR) industrial good practices to ensure that the desired actions are correctly performed. In addition, during normal situations, peer checks are available to ensure that correct actions are performed. However, during emergencies the STAR practice may not be performed and the peer checks may not be available. Therefore, action errors would rely on independent crew members (e.g., shift technical advisor) not typically having the responsibilities of peer review.

4.2 Task analysis and Crew Response Diagram (CRD)

The CRD is to graphically represent and document the critical tasks in a HFE. This step consists the following three stages:

Stage-1: Developing the CRD and its accompanying timeline
Stage-2: Identify critical tasks
Stage-3: Identify the error recovery paths

The IDHEAS methodology uses the crew response diagram (CRD) to document the above information. The CRD is an event sequence approach that starts with the first credible cue for the operator to perform the expected responses to succeed the HFE. Following the cue, the expected responses that all need to be succeeded in order to succeed the HFE are identified. These expected responses are represented as nodes in the CRD. Each nodes also is a branching point that has a success branch and a failure branch. The failure branch could lead to error recovery opportunities to bring the sequence back to the success track. The sequence of the expected responses is referred to as a success path. A HFE may have one or several alternative success paths.

4.2.1 Develop the crew response diagram and timeline

The objective of developing the CRD is to Identify the expected crew response paths within the HFE that lead to success. This includes providing information to understand the path progression, e.g., procedure transitions. There could be more than one paths with or without explicit procedure transition paths to succeed. HRA analysts should keep in mind that the essential objective of developing the CRD and task analysis is to estimate the likelihood that the HFE can be implemented successfully. Knowing each success path is beneficial for understanding the variations in performing the HFE. Trying to identify all possible paths (based on procedure instruction) may be time consuming, thus not practical for some PRA applications, and with potential of loss the big picture.

Additional information –

In the International HRA Benchmark study [NUREG/IA-0216, Vol.1], 14 crew performed a complex steam generator tube rupture (SGTR) scenario. This scenario starts with a

main steam line rupture event then following with a subsequent SGTR event. The timing of the SGTR was designed to occur after the MSIVs closure so there is no steamline radiation available (this is a misleading indication in this scenario). An HFE requires transferring to the E-3 procedure. In this experiment, 5 of the 14 crew transferred to E-3 based on the SG water level instructed by procedures; 8 out of the 14 crews transferred to the E-3 procedure was determined as knowledge-based (i.e., not relying on procedure instructions); and one crew is outlier who responded differently from others that resulted the main steamline radiation indication was available to this crew. The five crews entered E-3 based on procedure instruction were based on different procedure paths as below:

- *E-0 step 21 – ES-1.1 foldout page (two crews)*
- *E-0 step 24*
- *E-0 step 21 – ES-1.1 – E-0 step 19*
- *E-0 step 19*

This creates a dilemma that the knowledge-based actions are typically not credited in HRA when procedures are available. But without crediting the knowledge-based actions (decisions) the estimated HEPs could be significantly off from the true values. Fortunately, the situations are less likely to happen in less complex situations. The points are:

- *It is likely not practical to identify all procedure transition paths to succeed the HFE. Even though considered all the paths based on procedures could still miss the knowledge-based transition which in some situations could have significant effects on the analysis results.*
- *The HRA analysts need to make decision on the success paths to be modeled in the CRD based on the effort-and-benefit consideration.*

The following are the essential elements of performing Stage-1.

- **Identification of the operating procedures or operator training materials, as necessary that are applicable to this scenario.** The focus of this stage is to identify the procedures (titles and id's) and key parts of the procedures (foldout pages, and checklists, etc.) that guide the crew to respond to the situation. For example, a SGTR event, the response nodes could include: identifying the broken SG, isolating the broken SG(s), and depressurize and cooldown the RCS. **Determine the relevant cues and their timing.** Cues are the information to trigger operator's responses. Cues could be alarms, plant indications, field report, and procedure instructions, etc. Computer simulation of plant responses could provide the timing information of certain cues (e.g., tank water level is below certain threshold or pressure is exceeding certain level). The cues lead operator to enter the correct procedure(s) for the HFE are particularly important to be identified.
- **Identify the non-procedure prescribed responses lead to success.** In some cases, there is no written procedures suitable for the HFE. The operator would relies on their training, engineering judgment and skill-of-the-craft to implement the expected responses in the HFE. The identification of such responses requires understanding the systems and interviewing with operational staff.
- **Develop the timeline in parallel with the CRD.** In parallel with the development of the CRD, a timeline should be developed for each success path identified in the CRD, as necessary, to support assessment of the feasibility and error recovery of the responses. The CRD timeline indicates the expected time

of the occurrence of the plant cue (plant event) the completion of the previous event until the task shown and the completion of the crew tasks. The timeline could be critical to specify the PIFs statuses for the HEP estimates.

4.2.2 Stage-2: Identification and Definition of Critical Tasks

The purpose of this stage is to identify and analyze the tasks critical to the success of the HFE. Failure of any of these tasks will fail the HFE. When constructing a CRD, the critical tasks are represented under the CRD response nodes. The HEP of a HFE is the sum of the HEPs of all the critical tasks.

There is a considerable degree of flexibility regarding the number of nodes to be included in the CRD versus the numbers of critical tasks under the nodes. A node could include one or several critical tasks. There is a trade-off between the numbers of response nodes in the CRD and the number of critical tasks for each node. An analyst may choose to use every response node to represent only one critical task or to cluster several critical tasks in one response node.

Only the critical tasks modeled in the CRD will be analyzed and quantified for HEPs. A critical task is identified with the significant transition points in the response, such as entering a procedure, transitioning to another procedure, deciding to begin execution of actions. A critical task should meet all the following criteria:

1. *Task criticality* - The systems involved in the task are safety-critical, and the task involves changes to the operating configuration
2. *Task difficulty* - The task requires complex human involvement and has a good chance of human errors
3. *Recovery difficulty* - The consequences of the omitted or incorrectly performed task cannot be easily detected or corrected.

Additional information – The term "critical task" in traditional PRA

An HFE typically involves all macro-cognitive functions while critical task may only related to one or more macro-cognitive functions. This could differ from some PRA practice that some of the critical tasks are modeled as human top events (HFEs) in PRA event trees. HRA analysts need to aware the HFE and critical tasks as implemented in PRA may not be consistent with the instruction of this general methodology.

Identification of critical tasks begins with reviewing available procedures, guidelines, or instructions for the human response of the node. Each individual step in procedures or guidelines may be viewed as a subtask; subtasks may involve different cognitive activities, e.g., a step may direct the crew to collect information, to verify a plant status, to perform a plant state assessment, to make a decision such as transferring to another procedure or branch of a procedure, to execute the required manipulations. A critical task is identified by grouping the subtasks according to a common goal. In the case of no procedure available, critical tasks are identified by analyzing what operators have to perform in order to achieve the expected response.

Once the critical tasks are identified, detailed characterization of each critical task should be documented. Such information will be used the determination of CFMs and PIF status. Typical characterization should include the following:

- The goal (i.e., the success criteria) of the task
- The macro functions and activities involved:
- The requirements for the task such as: continuous monitoring of cues, use of secondary cues when the primary cues are not available, responding to key alarms, or implementing the responses within a certain time window, etc.
- The crew member responsible for the task
- Relationship to other tasks in the node
- Identification of needed tools and portable equipment.
- Other non-critical tasks that are performed by the same crew in parallel
- Interaction, communication, and coordination with other personnel.

4.2.3 Stage-3 Identification of Potential Recovery Opportunities

Each of the critical tasks represents an opportunity for failure. This is represented on the CRD as a downward arrow. The purpose of this stage is to explore the possibilities for recovery given a failure at one of the CRD nodes. This step identifies the opportunities for error correction, i.e. for recovery of the failure to correctly perform the task(s) represented by the node. Note however that per HRA convention, analysts may choose to assume that some actions will not fail and that there will not be a branching point. For example, Steps 1 to 4 of NPP procedure E-0 correspond to the immediate post-trip actions to verify reactor trip, turbine trip, power to the AC ESF busses, and the status of SI. Analysts may assume that these actions will succeed and therefore the node for E-0 "Reactor trip" does not include a failure path (branching point) and therefore recovery is not addressed.

The critical tasks represented in the CRD nodes include not only manipulation to systems but also information collection, assessment and decision-making. The opportunities for recovery can come from a number of sources. Information collection, assessment and decision-making are usually associated with a procedure entry, procedure transfer, or initiation of an action. No matter what the reason for failure at a node. The error correction opportunities relate to subsequent procedure steps conditional on the correct transition not being made (or steps in other applicable procedures) that have the potential for placing the crew on an alternative success path or that act as additional cues to perform the correct task or perform the correct procedure transfer. In addition, system conditions may evolve and generate new alarms or key parameter changes that crews would normally be monitoring and which would serve as cues for identifying the need for a different response.

For tasks involving manipulation of systems, the error correction opportunities will primarily arise from a monitoring activity that is capable of detecting that the plant is not responding as would be expected if the intended action had been completed correctly. These opportunities focus on the crew's detection and assessment of the plant feedback.

If opportunities are identified, they are represented as a dotted line for recovery leading back to the success path. However, it is important to note that the recovery nodes are not quantified separately. Rather, the recovery for a failure is addressed within the DTs when quantifying the relevant CFMs for a given node. Thus, the recovery nodes are illustrative of the recovery rather than a separate node for independent quantification.

The definition of the recovery nodes should document:

- The relevant procedural step(s)
- The crew member responsible for monitoring the plant status

- The information (e.g., cues/indicators) that is needed to be available to the operators for them to recognize the need for recovery
- The time of the cue and/or the time taken to reach the procedural step that indicates the need for recovery

This information will be used in the assessment of the potential for recovery. Part of this assessment is a determination of the feasibility of the recovery, e.g., whether the recovery opportunity occurs sufficiently early to allow time for the appropriate response to be executed. The recovery paths identified are graphically illustrated on the lower portion of the CRD. The supporting information for the recovery paths should be documented along with other characterization of the critical tasks.

Additional information – Recovery in performing NPP emergency operating procedures

Note that a recovery opportunity viewed in isolation is essentially another way of getting success, e.g., an emergency operating procedure (EOP) and a critical safety function status tree (CSFST) can both get to success. One concern is that an analyst might not know which order to consider them in, since the cue may be reached at the same time for both ways of getting success. This is an example of a modeling uncertainty. When analysts are uncertain as to how to model things, they make assumptions; in this case, an analyst might pick up the EOP cue as being the first, and the monitoring of the CFSFT criteria as a recovery opportunity. (One argument for this choice could be that the EOP is supposed to give the global picture of what's going on at the plant, whereas the CSFSTs, are as the name suggests, function oriented). Another analyst might choose to use the CSFST as the primary cue and the other one as the opportunity for recovery. This is not necessarily bad as long as the analysts have a reasonable argument as to why they chose to model it the way they did. The important thing is that both approaches have considered and identified all the options. In most cases, both should produce similar results and given the different ways of getting there in this case, the likelihood of failure, assuming there are no really bad PIFs, should be very small. If the analyst thought there might be a significant difference between the two strategies he/she could always do a sensitivity analysis.

In summary, CRD organizes the outcome of task analysis. The graphic representation of the CRD illustrates the success path, failure paths, and recovery paths. The supporting information for each CRD node should also be summarized and documented.

4.3 Analysis of time uncertainty

4.3.1 Treatment of the HEP contributed from time uncertainties

Time uncertainty analysis is to address the uncertainties in Time available (Ta), time before the plant reaches some undesirable state, and Time needed. i.e., how long it takes for specific automatic systems (or operator actions) to be successful in preventing the plant from reaching damage state. As long as recovery occurs before damage (i.e. if Tn < Ta), the plant is in a success state. Theoretically, when the crew has adequate time to perform tasks, the HEP is not affected by the time available except that longer time may yield more opportunities for recovering human errors and less time pressure on operators. However, we rarely know Ta and Tn precisely. There may be random factors that produce variability in these times as well as uncertainty in our knowledge of the processes involved. In other words, because of variability and uncertainty, nominally similar conditions could lead sometimes to success

and sometimes to failure. For example, there can be variability in the time required by different operating crews to complete the actions and there can be uncertainty associated with estimating the time required for the operator actions associated with an HFE. If the time available for a particular action is only somewhat longer than the time required, then the possibility arises that some crews might fail to complete the actions.
Therefore, assumes that the HEP of an HFE should consist two parts: the HEP caused by the time factor and the HEP calculated from the IDHEAS quantification model.

HEP = Pt + Pc

Pc – Probability of all the crew failure modes (for the selected DT path) of all the critical tasks of the HFE. This will be calculated from IDHEAS quantification model.
Pt – Error probability introduced by the time factor in the HFE. PRA seeks to determine the chance that recovery fails. **Pt** is denoted as the probability that the recovery time exceeds the time available for recovery. We represent our uncertainty by state-of-knowledge (probability) distributions.
To calculate **Pt** , We represent Tn in its probability density fuction f(Tn) and Ta in its probability densicy function f(Ta).Analysts need to estimate the distribution (central tendency and range) of time needed and time available. **Pt** is the convolution of the two distributions, i.e.,
.

$$\mathbf{Pt}(Tn > Ta) = \sum \text{Prob}\,[(Tn > Ta) \text{ and } (Tn = Ta)] = \sum P(Tn > Ta) \cdot P(Tn = Ta)$$

$$= \int_0^\infty (1 - F_\tau)(f_T \, dt)$$

4.3.2 Guidance on estimating distribution of time available

In the development of PRA event sequence models, success criteria are established for systems and components, and for specified operator (i.e. events explicitly shown in the plant event trees), that can prevent core damage or containment failure. Success criteria tell us the minimum equipment configuration required to ensure success of a given safety function for all credible conditions. Time available is the time before the plant reaches some undesirable state at which the success criteria could no longer be met. Realistic engineering models have been developed to examine many possible scenarios of starting conditions and equipment operability. Time available can be calculated a result of developing such detailed information. However, we can never know the available time exactly because of variability in plant conditions as well as uncertainty in our knowledge of the processes involved. This uncertainty is properly expressed as a probability distribution, fT.

The nuclear industry has been developing and elaborating computer codes which have permitted solution of many complex phenomena. Running the computer code against various combinations of plant and equipment conditions can be very resource demanding. On the other hand, many questions concerning event sequence timing are simple thermal-hydraulic problems. Often low-cost simple calculations would have adequately answered the question at hand, e.g. when will the pressurized water reactor (PWR) steam generators boil dry with no feedwater, or how long will it take to refill the pressurizer following a severe overcooling event? The analytic approach starts by reviewing the

preliminary risk results to identify the dominant risk contributors. Then analysts identify areas where it is important and justifiable to evaluate uncertainties or to 'sharpen the pencil' and perform more sophisticated analyses to better define success criteria. The goal is to understand safety quantitatively, not just to bound the results. Although the engineering analyses are 'best estimate' and deterministic is nature, there are physical and analytical uncertainties as well as operational variabilities no matter how sophisticated the analysis. Sensitivity studies permit to evaluate those uncertainties, as well as the variability associated with plant operation.

One example is the time available for the operators to establish bleed and feed cooling if no feedwater was available to the steam generators. The existing data show that, If the plant had been operating continuously for 18 months at full power, steam generator dryout would occur within about 1·5h. Had the plant been operating ng for only 1 month at full power, the time would be about 2 h. If the reactor was operating at less than full power, the time would be extended due to the reduced decay heat levels and the larger initial water inventory since the effective liquid density on the shell side of the steam generator bundle increases as power is reduced due to fewer steam voids.

4.3.3 Guidance on Estimation of Time Needed

NUREG-1852 and NUREG-1921 present a structured timeline to estimate time for an individual HFE (see Figure 4-1). This timeline is composed of several elements to capture the various aspects of time during the progression from initiating event until the time at which the action will no longer succeed.

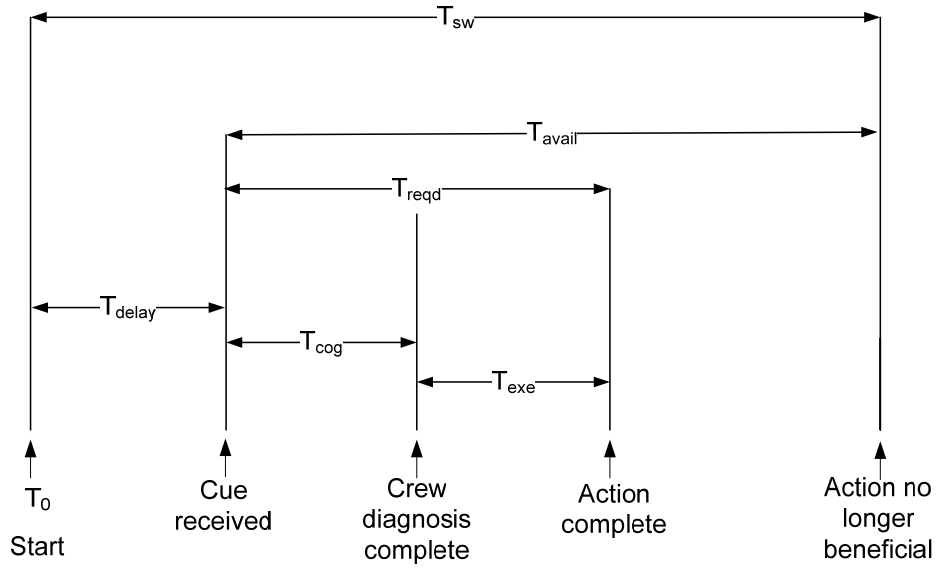


Figure 4-1 Timeline illustration diagram

The terms associated with each timing element are defined next and then further described in the subsequent text:

T_0 = start time = start of the event

T_{delay}= time delay = duration of time until the relevant cue for the action is received by the system and displayed to operators
T_{sw}= system time window
T_{avail}= time available = time available for action = (T_{sw} - T_{delay})
T_{cog}= cognition time consisting of detection, diagnosis, and decision making
T_{exe}= execution time including travel, collection of tools, donning of PPE, and manipulation of relevant equipment
T_{reqd}= time required = response time to accomplish the action = (T_{cog} + T_{exe})

Structuring the timeline in this way allows the analyst to demonstrate, among other things, the feasibility of the action from the perspective of timing. The operator action is feasible when the time available is greater than the time required. The time available (T_{avail}) consists of the system time window (T_{sw}) minus any time delays (T_{delay}), for example, time delay until the relevant cue for the action is received by the system and displayed to operators. The time required (T_{reqd}) consists of the time to recognize the needed action (T_{cog}) and the time to execute the action (T_{exe}); this is also called the *crew response time*. Each of the timing elements, including the start time, is defined next.

Start time. In Figure 4-1, T_0 is modeled as the start of the event, i.e., the occurrence of the initiating event, or the time of the demand for a function or piece of equipment which is unavailable/not responding.

System time window. T_{sw} is defined as the system time window and is the time from the start of the event until the action is no longer beneficial (typically when irreversible damage occurs, such as core or component damage). It is typically derived from thermal-hydraulic data and, for HRA quantification, is considered to be a static input. The system time window represents the maximum amount of time available for the action.

Delay time. T_{delay} represents the time from the start (typically the initiating event) until the time at which the system presents the cue to operators. It is also determined by the system and HSI design given the event. Yet, estimating T_{delay} should also consider unique event-specific uncertainties such as the nature of the initiator (fast or slow) or the sensor or detector response times. Potential delays that might be caused by operator actions or inaction due to the nature of the scenario should also be evaluated.

Cognition (diagnosis) time. T_{cog} is defined as the time for cognition and includes detection of the relevant cues, understanding/diagnosis, and decision making. It is best obtained by simulator observations or talk-throughs and/or walk-throughs. Yet, T_{cog} obtained through these methods may not be representative enough because various uncertainties and individual differences associated with T_{cog}. Therefore, we propose the following guidance on estimating T_{cog} when adequate observations are not available to verify or modify the observed T_{cog}, (i.e., when the observation sample is small or no observational results are available).

Execution time. T_{exe} is the time required for the execution of the action. *Execution time* is defined as the time it takes for the operators to execute the needed action(s) after successful diagnosis and decision-making. The execution time includes transit time to various areas in the MRC or to the local components, time to collect tools and don personnel protective equipment (PPE) if needed, and time to manipulate the MCR or local components. Useful inputs to develop T_{exe} can be obtained from observations of simulator data and walk-throughs or talk-throughs with the operators.

Guidance of estimating the distribution of time needed

Time needed includes T_{cog} and T_{exe}. Estimating T_{cog} should consider three key aspects: nominal contributors, uncertainty *factors*, and *bias factors (i.e., the information that may be missed due to the biases)*. We recommend the following process of estimating the probabilistic distribution of time needed:

Obtain an initial distribution of time including the central tendency and range (e.g., the 10^{th}, 25^{th}, 50^{th}, 75^{th}, and 10^{th} probability percentile). This information can be obtained through reviewing operational data, simulator data, and interviews with operators. HRA analysts should collect a range of times (using multiple independent estimates to the extent possible). Average crew response time for T_{exe} should be obtained, as well as an estimate of the time by which the slowest operating crews would be expected to complete the actions.

Calibrate the initial estimation by reviewing the factors contributing to time needed. For example, factors such as retrieving the tools needed or traveling to the site need to be included in T_{exe} when estimating time to lining up a pump. Tables 3-1 provides some typical contributing factors for T_{cog} and T_{exe}.

Modify the distribution by identifying and reviewing uncertainty factors that may change the time needed. For example, operators' familiarity with the scenario can significantly change T_{cog}. Tables 3-2 provides some typical uncertainty factors for T_{cog} and T_{exe}.

Verify the estimation by reviewing the bias factors that may occur in the estimation. Literature shows that estimation of time needed tends to be heuristic and various biases often result in underestimation. We provide some considerations of several common bias factors in time estimation based on cognitive literature.

Table 3-1 Factors contributing time needed

Cognitive task	**Factors contributing to time**
Detection	Travel to source location of information Prepare and calibrate equipment needed for detection Detect/attend to an indication; Confirm and verify the indicators Record and communicate the detected information
Diagnosis	Assess the information needed for diagnosis, such as knowledge and status of a valve, pump, heater, and battery, etc., integrate low-level information to create and/or determine high-level information; Identify plant status and/or conditions based on several parameters, symptoms and the associated knowledge, collect information and delineate complex information such as a mass and/or energy flow with which two or more system functions; Delineate conflicting information and unstable trends of parameters, e.g., interpret SG pressure trends when one train has failed; Wait for continuous or dynamic information from the system to complete diagnosis; Verify the diagnosis results or reach a team consensus
Decision-making	Prioritize goals. establish decision criteria, Collect, interpret and integrate data to satisfying decision Make decision – Determine on parameters, choose strategies or develop a plan Coordinate the decision-makers (especially with hierarchy of decision-making or distributed decision-making team) or achieve consensus needed for the decision Simulate or evaluate the outcome of decision
T_{exe} (Action)	Evaluate the action plan and coordinate staff. Travel and access to the action site; Time to acquire (deploy, install, calibrate) the tools and equipment (e.g., put on gloves) to perform the actions; Time needed for action implementation - Action steps, continuous action, and required timing of steps; Confirmation of the actions, waiting for system feedback

Table 3-2 Variability and uncertainty factors that modulate the time needed

Uncertainty factors	**Considerations**
Environmental factors	Radiation Weather Flood Fire Seismic
Plant condition	Multi-unit events Other on-going activities that compete resources
Work sites accessibility	Different paths to work site Continuous habituation Hurdles to access the work sites
Information availability	Visibility of information Familiarity with sources of information

Procedures / instructions applicability and training	Applicability of procedures or instructions Recent training
Decision-makers	Variability of decision-makers Variability in decision infrastructure Communication in distributed decision-making
Staff	Staff adequacy (e.g., whether other concurrent activities would reduce the staff available for the action, whether tasks can be performed concurrently with more than adequate staff) Command and control Staff experience (e.g., whether less-trained, non-regular staff is used)
Equipment, tools, parts, and keys	Familiarity with equipment Potential failure modes of equipment and recovery / backup
Scenario familiarity	Familiarity with scenario
Fatigue (mental and physical)	Time of the day Time on shift
Crew variability	
Others	

Additional information – Bias factors in time estimation

Anchoring bias. Estimation of time tends to be anchored at actual data obtained at a given situation without exploring the full range of possibilities.

Under representation/incomplete representation of the range of times. Estimating T_{cog} relies on subject matter experts' judgment or their calibration to simulator data. Given that great variability exists among individuals in completing tasks, HRA analysts should make efforts to ensure that the time estimated is representative of a normal operator population. In fact, when estimating T_{cog} and T_{exe} for assessing feasibility, when timing data are collected for crew response times, HRA analysts should strive to collect a range of times (using multiple independent estimates to the extent possible). Although an estimate of the average crew time for T_{cog} should be obtained, it is also critical to obtain an estimate of the time by which the slowest operating crews would be expected to complete T_{cog}, in other words, the maximum time it would be expected for all of the crews to complete T_{cog} under the conditions present in the scenario. Although the availability of training and operations staff may be limited, it is important to interview several trainers or operators for cases in which a small change in the time estimation could render a feasible operator action infeasible or significantly impact the resulting HEP. For actions that occur well after the initiating event or for actions with a long time window, a bounding estimate can often be useful.

Underestimation for complex scenarios. When estimating task completion time, people tend to focus on optimistic aspects of the scenarios and disregard pessimistic aspects, resulting in underestimation of time for complex scenarios. Therefore, analysts, in discussing the time required with trainers and operators, should thoroughly analyze the nominal contributors and modifying factors (see Table 2-1) involved in complex scenarios. In particular, the time required

to work through the relevant procedures (including consideration of the impact of verification steps that may not be critical to achieve the necessary actions but that nevertheless can require time) should be carefully evaluated (especially when operators are working with multiple procedures). The potential for operating crews to get stuck in a procedure while waiting for particular conditions or to have trouble transitioning to the correct procedure due to misleading or confusing indications should be evaluated.
Underestimation of the effects of interruption and workload. Cognitive studies demonstrated that the effect of interruption on task completion time is typically more severe than expected. Depending on types of tasks, interruption can result in 30-100% of increase in task completion time (without counting the interruption time). Analysts will need to discuss with the operators and trainers the types and likely occurrence of any potential interruptions that should occur given the scenario conditions and decide how much time should added in estimating the time required for T_{cog} (and T_{exe}). A related issue is that of workload. Activities that can slow crew response time such as peer-checking, routine monitoring, communication and coordination needed, responding to alarms, and other simultaneous or parallel activities that the crew would be expected to be involved in that could extend their response time should be included in estimating the time required. In other words, it shouldn't be assumed that the crews are only processing cues, stepping through the procedures, and taking actions.

In summary, this chapter provides guidance for HFE qualitative analysis. The analysis is for a given HFE. The input to the analysis includes the outcomes of scenario analysis and HFE definition; the output include the results of task analysis (CRD and its documentation) and the results of time uncertainty analysis; they will be used as the input to HEP quantification.

5 The basic Quantification Structure

HEP quantification is based on the notion that a critical task may have one or more failure modes and the likelihood of the failure mode is determined by PIFs. IDHEAS-G provides a basic Quantification Structure that consists of a set of basic cognitive failure modes (CFMs), cognitive mechanisms underlying the CFMs, and a comprehensive list of PIFs affecting the CFMs through the cognitive mechanisms. The Basic Quantification Structure is based on the Cognitive Basis for HRA in NUREG-2114. It is independent of HRA application domains. Application-specific HRA model can be developed from this generic structure.

5.1 Cognitive Basis for HRA

Human performs complex tasks through cognitive functions. Macrocognitive functions refer to the high-level mental activities that must be successfully accomplished to perform a task or achieve a goal in a naturalistic environment. The Cognitive Basis for HRA in NUREG-2114 is constructed on the five Macrocognitive functions: *Detection, Understanding, Decision-making (Response planning), Action execution, and Teamwork*. NUREG-2114 synthesizes cognitive findings, models, and theories about how the macrocognitve functions are achieved and infers the ways that these functions may fail (referred to as proximate causes). The cognitive basis includes the following information:

- How humans perform complex tasks - Cognitive functions
- How cognitive functions are achieved – cognitive processes
- How humans fail the cognitive functions – Proximate causes (i.e., failure of the cognitive process)
- What makes human reliably perform cognitive functions – Cognitive mechanisms
- What makes cognitive mechanisms fail and lead to proximate causes – PIFs

NUREG-2114 focuses on cognitive basis for operator tasks in NPP internal at-power operation, with the assumption that operators are well-trained crew, follow procedures, and perform tasks within control rooms. In order to build a cognitive basis for human tasks independent of applications and work domains, we performed extended literature review to develop a more complete set of cognitive processes, proximate causes, and cognitive mechanisms. Moreover, we reviewed literature and database about human errors in operating complex systems (e.g, aviation, space shuttle, chemical plants, NPPs, etc), and generalized the context characteristics, i.e., PIFs, that challenge the cognitive mechanisms and leads to failure of cognitive processes.

5.1.1 Detection

Detection is to perceive and recognize pertinent information in a complex work environment. In NPP, Detection is to perceive the plant abnormality. The perception of plant abnormal situation has sufficient strength to motivate the operator start to investigate and to understand the situation. The objectives of detecting abnormality can be one or several of the following cognitive tasks:

- Attend to salient information (Salient information pop out of complex scenes and attract personnel's attention)

- Check or acquire information directed by task goals
- Monitor system status or parameters (e.g., trends, abnormal signals)

Detection involves extracting information from complex work environment, such as checking the parameters on a control panel, monitoring parameters displayed on a computer screen, obtaining verbal reports from other personnel, and checking on system components. In a highly automated system, much of what operators do involves monitoring. Detection is the operator's recognition that something has changed (e.g., a component is not operating correctly), the value of a parameter has increased or decreased, or something is abnormal.

Cognitive process for Detection

In a naturalistic work environment, detection is not a snap-shot activity. It is an iterative process. Most detection activities are not passively responding to onset of the cues. Instead, detection typically involves operators actively seeking for cues or abnormality. This is true even for the objective of responding to alarm. Although alarms are salient enough to capture operators' attention and trigger the detection, in real operation, experienced operators have anticipation on what alarms might be coming up and they prepared to detect those alarms. Therefore, detection begins with knowing what information is to be detected. Similarly, perceiving the information is not the end of the detection function. Once the information is perceived, operators would verify the information; the verification is performed by self-checking, peer-checking, and super-visioning. Finally, since operators work as a team, the information from detection often needs to be communicated to other team members. In summary, the cognitive process for detection includes the following steps:

D1 - Establish the mental model and decision-criteria for information to be acquired
D2 - Preparation for detection
D3 - Select / identify / attend to sources of information
D4 - Perceive, register, and recognize information
D5 - Verify / modify detection
D6 - Retain / Document / Communicate the information

Here D1 through D4 are essential to achieve the objectives, and failure to perform any of these activities would result in failure of detection. D5 is to enhance the reliability of detection, and failure of D5 increase the likelihood of detection failure. D6 is critical to the success of detection when the task requires to record or communicate the detection results.

Proximate causes

The failure of the steps of the cognitive process for Detection is the first direct cause to the failure of the function. Such failures are referred to as proximate causes (PCs). The PCs for Detection are the following:

- No or wrong mental model for detection
- Wrong equipment for detection
- Information not attended to
- Information not perceived or misperceived
- Information incorrectly recognized, interpreted, or classified
- Fail to communicate or record the information

Cognitive mechanisms

The literature review report identified the following cognitive mechanisms:

- Perception of sensory information: The basic process of perceiving sensory information.
- Vigilance: The alertness of the brain is necessary for continuously perceiving information, monitoring, focusing attention, and retaining information in working memory.
- Information foliage: The process of filtering out irrelevant information and detecting salient changes in the environment
- Attention: A control mechanism for selecting pertinent information
- Working memory: A control mechanism that retains the perceived information and also retains the objects to be monitored or searched.
- Expectation and executive control: A control mechanism that guides the detection to the outcome of the task goal/objectives (i.e., "you see what you are looking for."). Unexpected information is less sensitive to the detection process. The brain's executive control terminates a detection process upon the condition that the expected information is detected.

Xing et al (2011) synthesized the cognitive literature on human errors and proposed a cognitive model of human error causes in complex tasks. The model consists of four notions that were the synthesis of many neurophysiological and psychological findings:

i) Cognitive mechanisms have capacity limits or vulnerabilities; task demanding that reaches or exceeds the limits can result in performance errors;
ii) Experienced domain experts develop and intentionally use various barriers (individual's experience, procedures, HSI, etc) to cope with the vulnerabilities to reliably perform complex tasks;
iii) Cognitive limits and the effectiveness of the barriers can be impaired by personnel factors such as fatigue, stress, and drug/alcohol abuse; and
iv) Rare errors occur when the task demanding reaches or exceeds some cognitive limits while the barriers are not fully effective or not used.

The cognitive limits and vulnerabilities establish the boundary condition under which a cognitive function can be reliably achieved. Failure to meet a boundary condition is typically referred to as error causes in cognitive literature. Below are some examples of the boundary conditions:

- Visual adaption/attenuation: The activities of the visual system are reduced over time with continuous or repetitive activities.
- Information quality for segmentation/pop-out: Visual cues have to be salient enough to pop out from a complex scene to enter the attentive perception stage.
- Limited capacity of the attentive stage: While the pre-attentive stage processes information within a view angle of ~120°; the attentive stage only processes foveal information within a view angle of 2° to 4°. Thus, information that did not come from the fovea is unlikely to be noticed.
- Perceptual bias: The binding of visual features into an integrated pattern/object and their recognition are influenced by prior visual experience (e.g., "You see a cat because you know what a cat is"). However, experience can bias object recognition.
- Working memory: Working memory for visual search/monitoring has a capacity limit of three to four items. Items in working memory need to be attended frequently before they fail in memory. It takes 0.5 to 4 seconds for perceived information to be reliably stored in working memory.
- Inattentional blindness: While attention is a critical mechanism to ensure that salient information is processed in a timely manner, inattentional blindness is the failure to notice an unexpected but fully visible object while the attention is focused on another task, event, or object. This is similar to the concept of "tunnel vision."

From the literature, we synthesized the findings about boundary conditions of the cognitive mechanisms. These boundary conditions are later used to identify PIFs that challenge the capacity limits of the cognitive mechanisms. Below are some example boundary conditions:

Perception –
- The signal (information to be detected) is absent or too weak to be perceived
- The signal is ambiguous thus perceived incorrectly

Vigilance -
- Vigilance is reduced after sustained cognitive activities
- Vigilance is attenuated after a sustained "no signal" period

Information foliage –
- Failure to automatically detect the signal (alerts or alarms) because the signal is not salient enough to pop-out of the complex environment.
- Failure to select out irrelevant information due to information overload or not well organized

Attention –
- Failure to focus attention at the expected signal
- Failure to maintain sustained attention
- Failure to shift attention

Working memory –
- Working memory overflows (i.e., exceeding the working memory capacity)
- Working memory fades over time

- Working memory is interfered by interruption/disruption.
- Working memory for one task is confused with the memory for another task.

Expectation –

- Wrong expectation (i.e., bias) leads to missing pertinent information
- Narrowly focused expectation leads to missing relevant information
- Failure to adjust the expectation based on situation.
- Failure to meet the task goal/objective because of ambiguous expectation (e.g., premature termination of detection process)

5.1.2 Understanding

The Understanding macrocognitive function is to integrate pieces of the detected information with one's mental model of the task context to generate awareness of the situation and diagnose problems. In NPPs, Understanding is to generate the correct assessment of the plant status for response planning. The cognitive tasks under this function includes:

- Establish situational awareness
- Evaluate criteria
- Diagnose the problems (e.g., conflicting information, missed or misleading information)
- Make predictions and expectations for the upcoming situation development

Understanding is the evaluation of current conditions to determine if they are within acceptable limits, or to identify the underlying causes of any abnormalities. Operators actively try to construct a coherent, logical explanation to account for their observations. The function *Understanding* involves two related concepts: the situational model and the mental model. The mental model consists of the operator's internal representation of the physical and functional characteristics of the plant and its operation, as they understand it should be. This model rests upon formal education, training, and experience. Situation assessment occurs when operators use their mental model to understand information they obtained. The cognitive representation resulting from situation assessment is termed the "situation model," which refers to the understanding that personnel have of the plant's current situation, (i.e., their current situation model). To construct a situation model, operators use their general knowledge and understanding about the plant and its operation to interpret their observations and to extract its implications. Limitations in knowledge or in current information may entail incomplete or inaccurate situation models. General knowledge about human performance, the so-called "mental model" consists of the operator's internal representation of the physical and functional characteristics of the plant and its operation as they understand it should be. The mental model rests on formal education, training, and experience.

Cognitive process and proximate causes for Understanding

The cognitive process for understanding includes the following steps:

U1 - Assess/select data
U-2 Select / adapt / develop the mental model
U-3 Integrate data with mental model to generate understanding (situation awareness, diagnosis, resolving conflicts))
U-4 Verify and revise the understanding

U-5 Communicate the outcome with other parties

Correspondingly, the proximate causes for failure of Understanding are the follows:

- Incorrect data
- Incorrect mental model
- Incorrect understanding (i.e., incorrect integration of data and mental model)
- Early termination of the iteration process of Understanding
- Failure of communicating the outcome of Understanding

5.1.3 Decision-making

Decision-making is to decide upon actions to resolve the current situation. In NPP, Decision-making is primarily for response planning. Response planning is to layout the required activities to properly address the perceived plant status as a result of the diagnosis process. Depending upon the situation, the operator may need to adjust the response planning to address the situation dynamics. The cognitive tasks under Decision-making include:

- Make selection among multiple options or strategies
- Determine or develop new configuration or changes of existing ones (e.g., changes of personnel, strategies, criteria, goals, etc)
- Make GO/NO-GO choice
- Make plans

Cognitive process of Decision-making and proximate causes

DM1 – Manage the goal
DM2 – Select or develop a decision model to meet the decision goals and criteria
DM3 – Acquire / select information to be used for DM
DM4 - Make decision (judgment, strategies, plans)
DM5 - Simulate / evaluate the decision / plan
DM6 - Communicate and authorize the decision

The corresponding proximate causes are:

- Incorrect Goals or Priorities Set.
- Inappropriate decision model
- Information is under- represented
- Incorrect Internal Pattern Matching.
- Incorrect Mental Simulation or Evaluation of Options
- Decision is not properly communicated

5.1.4 Action execution

The action is to implement the response plan as specified by the response planning macrocognitive function. In this report, action refers to the physical actions that operators perform on the human system interface to interfere with the scenario's course. There are many

ways of classifying cognitive tasks under Action execution; the most straightforward one is the following:

- Execute simple actions (e.g., manipulate a control, record information, provide control inputs)
- Execute complex, logic actions (multiple steps, spatially and/or temporally distributed, with logic conditions, or continuous control)

Cognitive process of Action execution and proximate causes

The cognitive process for Action execution includes the following steps
E1–Assess action plan
E2 - Develop / modify action scripts
E3– Synchronize, coordinate, and prepare for action implementation
E4 - Implement action scripts
E5 - Verify and adjust actions

The corresponding proximate causes are

- Fail to assess action plan
- Action scripts or procedures not available or applicable
- Fail to perform planned action
- Fail to coordinate action implementation
- Fail to verify action outcomes

5.1.5 Teamwork

Teamwork is a macrocognitve function that is achieved through other macrocognitve functions and it binds other macrocogntive functions together. Teamwork is to communicate information, collaboratively carry out tasks to complete tasks in a timely fashion, and to coordinate with others to achieve the tasks more reliably than performed by an individual. Communication is information exchanged between crew members or between crew and machine systems. It include Initiating assertiveness (i.e., communicating ideas and observations in a manner which is persuasive to other team members), exchanging information (clearly and accurately, and confirm information. For NPP control room operation, the communication is primarily three-way communication between operators. For external events and severe accident management, communications may include less-procedural protocols and involve using machine systems (e.g., computers, wireless phones, etc). Coordination is to maintain a big picture of the situation to oversee the crew responses to the situation to ensure all aspects of considerations (e.g., technical specifications) are properly addressed to prevent overlooking of important risk items. Coordination includes Prioritizing and coordinating tasks and resources, reacting flexibly to

changing requirements of a task or situation, and giving help to other team members in situations in which it was thought they need assistance. Collaboration is to provide infrastructures and instructions and monitor crew activities in response to situations. Collaboration ensures that personnel activities are properly authorized and implemented, and rules and regulations are enforced. Collaboration includes performing leadership ((directing and coordinating the activities of, and motivating other team members, assessing team performance, and establishing a positive atmosphere), cooperating two or more team members on a task which requires meaningful task interdependence without any leadership, and co-operating in the accomplishment of a task as directed by a more senior team member.

Typical teamwork behaviors include adaptability, shared situational awareness, mutual performance monitoring, motivating team members/team leadership, mission analysis, sharing information, team decision-making, assertiveness, interpersonal relations, and conflict resolution. These behaviors are achieved through other four macrocognitve functions. Teamwork provides an infrastructure for crew to work as a team, yet ultimately every teamwork objective is achieved through individual cognitive functions. Therefore, the cognitive process for teamwork resides in the cognitive processes of all the four individual cognitive functions.

Additional information: Teamwork in NPP control room operation

Communication

In normal situations, three-way communication is required for control room operations. This may not happen or is conducted in an inconsistent manner in response to an emergency event. Between the control room crew members, except the typical three-way communication between the control room supervisor and the reactor operators to implement operating procedures, crew updates and crew briefs are two types of common communication. Crew updates are performed to update the operating crew of plant status. The initiating individual would announce "crew update", and the other crew members are expected to reply "update" immediately and silently wait for update. Then the initiating individual would announce the new plant status (e.g., certain parameters exceed a certain threshold) then announce "update complete" to finish the update. A crew update typically takes less than 15 seconds. Crew briefs, typically initiated by the control room supervisor, are used in the situations such as transferring to another procedure to obtain input about the decision. In this case, every crew member needs to reply (e.g., agree to transfer to the procedure). In situations that the shift manager determines a need to regroup the crew in response to the event, the shift manager would call for a crew briefing to discuss current situation and identify the areas requiring more attention. Therefore, crew briefings are longer than crew updates. The briefing time could vary significantly from situation to situation.

Communication between the control room crew and onsite crew (and security) typically requires communication equipment. Multiple types of communication equipment are available such as phone and radio. In most cases, the control room is the communication center. Onsite information such as fire, chemical spill, and personnel injury will be reported to the main control room. If the situation is an emergency, the onsite personnel would call to the emergency line to have the control room operators' immediate attention. However, protecting reactor safety has higher priority than answering emergency phone calls. So if the emergency phone call occurs at the same time that the control room operators are performing emergency actions (e.g., the post reactor trip immediate actions) then the operators are not expected to answer the phone call until operators are available. If offsite assistance is required (e.g., ambulance, fire truck, or

helicopter) the control room would call the corresponding organizations for assistance. In the situations in which the emergency response organization is mobilized, communication is an important to coordinate the control room, technical support center (TSC), and operation support center (OSC) work.

Coordination

At a glance, the control room crew composition and responsibilities reflect a team work concept. A typical control crew consists of a control room supervisor, board operators (e.g., reactor operator and balance of plant operators), auxiliary operator, technical shift supervisor, and shift manager. The staffing and composition provide capacities for peer checking and performing simultaneous multiple tasks demand. During emergency situations, the control room supervisor works with the board operators to implement procedures to protect plant safety. The auxiliary operator shares the board operators' workload by typically performing procedure attachment instructions. The shift technical advisor performs independent plant status assessment as an independent check to the direction led by the control room supervisor in handling the event. The shift manager provides oversight of the control room activities. During an event, the control room supervisor works with the board operators using three-way communication in implementing the procedure instructions. This work is a small unit of team work. In a fire event, a control room operator works with the onsite fire brigade to implement the fire procedure using radio equipment for communication. This is another example of team work.

Typically an operating crew is trained together and works on shift together. However, reasons such as taking vacation, sickness, family emergency, or temporary personnel re-arrangement (e.g., preparing for refueling outage) could have crew members not typically trained together to be on shift together. The crew familiarity with each other may affect certain crew behaviors and in turn affect crew performance. For example, crew updates and crew briefs are important means to keep crew consensus on plant status and the strategy employed to handle situations. Having the right frequency and timing of crew updates and crew briefs significantly improves crew efficiency.

In severe accident situations, teamwork between the control room, TSC, OSC, and emergency response facilities would significantly affect overall performance in mitigating the event. Examples such as transferring the overall decision-making responsibility from the control room to TSC, managing a large number of supporting personnel with different responsibilities, and working with offsite fire fighting support represent challenges to teamwork.

Collaboration

Collaboration in control rooms is mainly achieved through procedures and crew infrastructure, and supervisors are in charge of collaboration. The control room crew provides two different levels of supervision. The control room supervisor supervises the board operators, and the shift manager supervises the overall control room activities. If the emergency response organization is mobilized, the TSC oversees the overall emergency responses. The supervisors need to maintain a big picture knowing the situation, the current status of responses, and the direction of future responses to ensure that no important safety issues are omitted and the event is handled in an optimal way. The shift manager has the responsibility of supervising the overall control room activities. During emergency situations the control room crew could form sub-work groups to simultaneously handle multiple concurrent tasks (e.g., internal event with concurrent fire event). The shift manager oversees the concurrent control room activities and ensures that the technical specifications are properly implemented. If the control room activities are incoherent, lost direction, or other reasons that require a re-grouping, the shift manager has the responsibility to call for a crew brief. Supervision is an art to maintain balance between letting

the crew handle their tasks and interrupting the crew activities to refresh their focus. In performing this, the supervisor needs to have an open mind to take input from the crew members for decision considerations.

5.2 The Basic quantification structure

The Quantification Structure is the basis for application-specific quantification models and is application-independent. It consists four parts: HEP quantification formula, a basic set of cognition-based crew failure modes (CFMs), a comprehensive list of PIF characteristics, and a list of cognitive mechanisms that link the CFMs and PIFs (i.e., the mechanisms about why a PIFs leads to the CFM).

5.2.1 HEP quantification formula

The HEP of a HFE includes the error probability contributed from time uncertainties (Pt) and the error probability contributed from the cognitive failure modes. The task analysis identifies critical tasks in a HFE. The HEP of a critical task is the joint of the HEPs of the CFMs applicable to the task; the CFM contribution to the HEP of a HFE is the sum of HEPs of all the critical tasks. These can be written in the following formula:

P = Pt + ∑ (1-P1)(1-p2)(1-p3)….

Pt – Error probability introduced by the time factor in the HFE

P1, P2, P3, P_i – Probability of a crew failure mode for a given critical task.

When the probabilities of CFMs are general small, the formula can be simplified as:

P = Pt + ∑ (∑ P_i)

5.2.2 Crew failure modes

The Quantification Structure describes crew failures at two levels of details.

The high-level Cognitive failures:

The cognitive failure modes are based on the failure of the four macrocognitive functions. Four failure modes are defined:

- Failure of detecting information
- Failure of Understanding and assessing situation
- Failure of making decisions or planning actions
- Failure of executing planned actions

The detailed cognitive failure modes (CFMs)

While the proximate causes represent the ways that the internal process of achieving a macrocognitive function may breakdown, detailed CFMs represent the ways in which failures would be manifested to an outside observer watching the crew with an understanding of what it is the crew should be doing in response to an upset condition. In other words, CFMs represent the behaviorally observable ways of proximate causes occurring. IDHEAS identifies critical

tasks performed by a crew to achieve the expected human response in an HFE; a critical task may involve one or several macrocognitve functions and each function may have one or multiple failure modes. Therefore, two basic requirements for a basic set of CFMs are 1) the CFMs form a complete representation of the macrocognitve functions and 2) the CFMs shall be non-overlapping - it means that the scopes of the CFMs do not overlap with each other therefore the kinds of crew failures represented by one CFM will not be represented by any other CFMs. Thus, any potential crew failure will be counted only once when the failure probability is estimated. Given that the macrocognitive functions and there process steps are not independent, i.e., the success of a function or process step depends on preceding functions / steps, the CFMs need to be defined against artificial boundaries in order to be non-overlapping.

Our goal for developing a basic set of CFMs is to construct a set of behaviorally observable CFMs that is the complete representations of all the PCs and define the CFMs in a way that they are non-overlapping or mutually exclusive (i.e., only one of the mutually exclusive CFMs can be selected for a given critical task). In principle, a process step or PC can be divided into three CFMs:
The activity defined in the step is omitted
The activity defined in the step is not achievable
The activity defined in the step is performed incorrectly

While a PC can always be divided into these three kinds of CFMs, some PCs may only have one or two types of CFMs applicable. On the other hand, one of the CFM types may be further divided into subtype to better represent the observable behaviors. Below are some examples for these situations:

Example 1 - Process step D1 for Detection is "initiate detection - Establish the mental model and decision-criteria for information to be acquired," the corresponding PC is "fail to Establish the mental model and decision-criteria." The PC can be represented by three CFMs:

- D1-1 Detection for the right information not initiated (e.g., Skip steps of procedures for detection, forget to check information, not realize to check the information, not check the right information)
- D1-2 Failure to prioritize information to be detected
- D1-3 Wrong detection criteria were used

Here D1-1 is for the CFM type "The activity defined in the step is omitted"; D1-2 is for the CFM type "The activity defined in the step is not achievable"; D1-3 is for the CFM type "The activity defined in the step is performed incorrectly."

Example 2 - Process step D3 is "Identify and attended to sources of information," and the corresponding proximate cause is "fail to attend the source of information." The PC can be divided into two CFMs:

- D3-1 Fail to access the source of information (fail to access, view, or measure partial or all sources, motor failure in probe movement to sub-areas for detection)
- D3-2 Wrong source attended

D3-1 represents the CFM type "The activity defined in the step is not achievable"; D3-2 is for the CFM type "The activity defined in the step is performed incorrectly." The CFM type "The

activity defined in the step is omitted" is already represented by the CFMs in D1 " Initiate detection."

Example 3 - Process step D4 is "Perceive information" and the corresponding PC is "fail to perceive the information." This PC is divided into five CFMs

- D4-1 Key alarm or alert not attended to
- D4-2 Fail to recognize that primary cue for information is misleading (e.g., wrong information due to sensor or indicator failure)
- D4-3 Key parts of information (abnormals) not perceived
- D4-4 Information misperceived (information Incorrectly perceived, fail to perceive weak signals, reading errors)
- D4-5 Fail to monitor status (e.g., Information or parameters not monitored at proper frequency or for an adequate period of time, fail to monitor all the key parameters)

The CFMs represents different detection activities: responding to alarms or alerts, checking information, and monitoring system status. D4-1 represents the failure of responding to key alarms; D4-2, D4-3, and D4-4 are for checking information, and D5 is for monitoring status. The three basic types of CFMs are either embedded in these CFMs or not applicable for the activities defined in process step D4.

Example 4 - The process step E4 for Action execution is "Implement action scripts" and the corresponding PC is "*Failed to correctly perform the planned action."* This PC is divided into two groups CFMs:

- E4-1 Fail to follow procedures (e.g., Skip steps in procedures)
- E4-2A Fail to execute procedulized simple action
- E4-2B Fail to execute procedulized complex action (e.g., Execute all the steps of a complex action in wrong timing or sequence, Execute actions that do not meet the entry conditions, Not or mis-coordinate execution of complex actions among team members)
- E4-2C Fail to execute procedulized control actions
- E4-3 Fail to execute skill-of-craft actions
- E4-4 Fail to execute non-continuous long-lasting actions

The CFM types "The activity defined in the step is not achievable" and "The activity defined in the step is omitted" are represented by other CFMs of preceding steps of the Action execution process. Here the CFM E4-1, 2, 3, and 4 are all for the CFM type "The activity defined in the step is performed incorrectly." E4-1 and E4-2 are for procedulized actions. Notice that E4-2 has three options each modeling a different type of procedulized action, thus E4-2A, E4-2B, and E4-2C are alternative and only one of them can be selected for a given critical task. E4-3 is for skill-of-craft actions that are not specified and practiced in detailed procedures. E4-4 is for actions that last multiple hours or days and some action steps are performed intermitted with hours apart.

Appendix A shows the full set of CFMs identified for the Basic Quantification Structure. The CFMs are organized by the macrocognitive functions and proximate causes. Each CFM represents a group of behaviors that fall in the CFM scope. We provides one or several example behaviors for some CFMs to demonstrate the meaning of the CFM. For example, the CFM D4-5

"Fail to monitor status" can include the behaviors such as information or parameters not monitored at proper frequency or for an adequate period of time or failing to monitor all the key parameters. These behaviors can also be viewed as subtypes of the CFM.

5.3 Cognitive mechanisms for CFMs

NUREG-2114 and our additional literature review synthesize the cognitive mechanisms underlying the macrocognitive functions. Human makes errors because of the capability limits and vulnerabilities of mechanisms. NUREG-2114 describes the negates of the mechanisms. The Basic Quantification Structure includes the cognitive mechanisms. Moreover, we infer the links between the mechanisms and CFMs of a PC. The linked mechanisms to the CFMs of PC explains why and how CFMs occur. PIFs are the factors that make the task challenges the capacity limits or vulnerabilities of the mechanisms. Thus, the cognitive mechanisms associated with each PC/CFM forms the foundation of identifying PIFs relevant to the CFMs. The cognitive mechanisms also help HRA analysts to better understand the CFMs and PIFs when developing and applying a quantification model from the Basic Quantification Structure.

Appendix A documents the cognitive mechanisms and their links to every PC/CFM for the four macrocognitive functions.

5.4 PIFs affecting HEPs

5.4.1 Overview of PIFs

The CFMs, i.e., the various types of failures of the cognitive functions, occur as a result of breakdown of one or several cognitive mechanisms. For example, the CFM, *Key Alarm Not Attended to*, can be caused by a loss of vigilance, lack of attention, or memory overload. The breakdown of cognitive mechanisms is caused by factors like task demands, inadequate job aids, or individual abilities to perform the tasks. Such factors are referred to as performance influencing factors (PIFs) in HRA. The Basic Quantification Structure models the following categories of performance influencing factors (PIFs):

- System – scenario, system responses, information available to crew
- Crew – staffing, work environment, work process (e.g., command and control, authorization, infrastructure for coordination and cooperation), organizational factors, stress and pressure, fatigue and fitness-for-duty.
- Task – workload, criteria and special requirements for tasks
- Crew factors – human-system interface (HSI), tools, procedures, training, experience,

The General Methodology models these PIF categories through the detailed traits or aspects of a high level PIFs. For examples, some PIFs in the HSI category are alarm saliency, distribution of relevant information, display format; PIFs for the training category include perceived urgency of a human response, frequency of training, special training on instrument failure modes.

The Cognitive Basis Structure provides the links between CFMs and cognitive mechanisms. Using that as the basis, we reviewed the literature, human event or accident reports, and human error databases of different work domains (e.g., nuclear, medical, aviation) to identify PIFs for every PC and CFMs. As the result, a comprehensive PIF list is developed. The PIF list has the following features:

1) Every PC and its CFMs are associated with a set of relevant PIFs;

2) Each PIF influences the CFM through one or several cognitive mechanisms
3) Each PIF has been notified in one or more scientific papers, event or accident reports, and/or human event databases
4) Every cognitive mechanism for a PC /CFM is linked to one or more its PIFs
5) All the PIF in existing HRA methods are represented by the PIFs in the list, although not in a one-to-one mapping.

The PIF list is not exhaustive and should be a living document, as new PIFs can appear in various work domains. For example, NPP control room upgrading to digital instrument and control may introduce new PIFs or modify the ways the PIF affect human performance. The Basic Quantification Structure makes it easy to add new PIFs to the existing structure.

5.4.2 The General PIF - Workload

Workload is a PIF in all HRA methods. In fact, the terms workload, taskload, and task complexity have been used to refer same or overlapping content in HRA. There are also many different definitions or measures of workload in cognitive literature. In HRA, workload is referred to the task features that impose cognitive resource demands approaching to or exceeding human's cognitive capacity limits. IDHEAS-G identified the following seven workload factors:

Unfamiliar / unusual scenarios – Handling unfamiliar scenarios requires complex and sustained cognitive activities. Unfamiliar scenario typically imposes challenges for crew to understand the situation and make the right decisions. In addition, operator responses could be slower and with greater uncertainty for unfamiliar scenarios comparing to familiar scenarios. In unfamiliar scenarios, the situation-specific tasks may not be explicitly identified in the procedures but rather need engineering judgment.

- Multitasking – Multitasking refers to performing parallel and intermingled cognitive activities. Because each task requires multiple cognitive functions such as detecting cues/parameters, comparing and assessing information, programming and executing sequences of actions, operators have to frequently switch between these tasks for multitasking. Frequent switch of cognitive function is err pron. A typical example of multitasking is that the crew implements concurrent procedures and procedure attachments in parallel to the main procedures; an extreme example of multitasking is that decision-makers have to handle several units that are under different critical situations.
- Frequent or persistent distraction and interruption – Distraction and interruption refer to non-critical or non-procedural tasks that are added to operators while they are performing critical tasks. Examples of distraction are answering phone calls, being requested to provide information, being distracted by other things going on in the work environment. High distraction / interruption refers to the situations that operators are distracted/interrupted for a prolonged period of time (e.g., longer than 2 minutes) or interrupted by cognitive-demanding tasks and requests.
- Unpredictable dynamics – This refers to a situation where system responses differs from what is expected by the crew and procedures (scenario-procedure mismatch), or in a fast pace scenario progression situation where the scenario could significant changes in a short time that require the operator constant monitoring to respond promptly. In some situations, the operators may need to monitor multiple parameters, perform mental calculation or simulation to have a holistic understanding of the situation and decide appropriate responses.
- Task complexity –

- Time pressure and other stresses- Time pressure refers to the sense of time urgency perceived by an operator to complete a task. This sense of time urgency creates a psychological pressure (time pressure) affecting the operator's responses such as making trade-off between the thoroughness in performing the task and completing the task in time. Because the time pressure is based on the operators' perception and understanding of the situation that may or may not be truly reflect the actual situation. Therefore, time pressure is most likely to occur when there is marginal time or inadequate time available, it also could occur in the scenarios with luxury or adequate available time if the individuals have an incorrect understanding. Other stresses and anxieties such as concern for families in emergency conditions, fear of potential consequences of plant damage, and worrying about personnel safety can also impact performance.
- Mental fatigue – Mental fatigue can be caused by long non-routine, stressful working hours, or right after a high cognitive demanding period. Mental fatigue leads to loss of vigilance, difficulty in maintaining attention, and reduced working memory span. Human tends to use heuristics (short-cut) in situation assessment and decision-making.

All the seven factors challenge one or several key cognitive mechanisms: Central executive, Working memory, and attention. These mechanisms are essential to all the Macrocognitve functions, although the quantitative effect may vary between the functions. Also, the factors can potentially affect the entire cognitive process of every macrocognitve function, thus they are not linked to any specific PCs.

Additional information – identifying and defining workload factors
The workload factors were identified and defined through a literature study and discussion with a group of subject matter experts in NPP operation. There are many definitions and measures for workload in the literature. For example, many human factors studies use amount of work to be done with a given period of time as a workload measure. However, this kind of workload do not affect the likelihood of human errors as long as the time available is adequate for the work. We synthesized seven workload factors that can challenge the capacity limits of cognitive mechanisms, and refine the definition of these factors through discussion with the subject matter experts. The experts came up with operational examples of how each factor may affect performance and increase the chances of errors.

5.4.3 Two types of PIFs

The human error probability (HEP) for a given CFM is determined by the status of the PIFs associated to the CFM. A PIF in its nominal, expected status does not increase the likelihood of a CFM, while a PIF in a poor status adversely impacts task performance, challenges the cognitive mechanisms, and increases the likelihood of the CFM. Existing HRA methods model PIFs as a binary or step function for simplification. In reality, the relation between a PIF status and the HEP of its relevant CFM is typically a non-linear, continuous function. We synthesized the finding about the effect of the PIFs on CFMs. For example, experiments and operational data analysis [**ref] showed that the human error rate does not change for task complexity below a certain threshold, increases linearly with task complexity above the threshold, and

increase exponentially with very high task complexity. The synthesized information is documented in a separate report [ref**].

Through the review of PIFs effects, we found that there are two intrinsically different types of PIFs. One type of PIFs directly contribute to the HEPs; a single PIF can change the HEP across a range of several orders. For example, experiments showed that using two information displays with low and high accuracies of information used for situation assessment (i.e., the Understanding macrocognitve function) resulted human error rates from 0.05 to 0.8 [ref**]. Such PIFs are related to the quality of the inputs needed for a macrocognitive function, or the specify of criteria by which the task is judged as correctly performed. This finding is consistent with the Signal Detection Theory stating that the likelihood of human errors is determined by information sensitivity (i.e., the quality) and the criteria for information process [ref**]. We refer such PIFs as to HEP contributing factors. The other type of PIFs modifies HEP in a relatively small range, typically less than a factor of 10 between the nominal and very poor status of a PIF; also these PIFs alone usually do not lead to human errors. For example, time pressure can increase the likelihood of errors, but the factor alone usually does not cause errors if other PIFs are in nominal status. We refer such PIFs as HEP modification factors.

Appendix B presents all the PIFs along with their associated PC/CFMs and cognitive mechanisms. For every macorcognitve function, the first section of the PIFs are HEP contributing factors that directly contribute to the HEP of the function; the next section are the workload factors that apply to all the CFMs; the last section are the PIFs specific for every PC and its CFMs.

In summary, the Basic Quantification Structure provides a comprehensive set of PIFs for each macrocognitive function. These PIFs cover the context of system, crew, and tasks. The definitions of the PIFs are human-centered and system-neutral so they can be applied to various NRC HRA applications such reactor operation, spent fuel pool, dry casks, and radioactive medicine; existing and new reactor; before and after core damage; actions taken place inside and outside of the main control room, and internal events and external events, etc.). For a specific application, the HRA analysts may exclude the PIFs not relevant to the application. For example, for a PRA level-1, internal event, inside the MCR action, most environmental factors have negligible effect on human errors. Therefore, the PIF list can be viewed as a grand pool of PIFs that can spin to subsets for different HRA applications. The next chapter will present the guidance on developing application-specific quantification models from the Basic Quantification Structure.

Additional information - PIF considerations for NPP applications

This section documents some our considerations on PIFs for NPP operation. The information is intended to facilitate readers' understanding of PIFs through examples in a specific application.

PIF consideration for Detection

Detecting a piece of information typically needs the following information:

- *Opportunities the information could be perceived: for the information displayed only in a location not constantly monitored, the opportunities when the information could be detected. For example, most information are available all*

time in the MCR but some information may only be detected during shift turnover plant walkdown or during refueling outage.

- *The location of the information source: To check a control room indication, the information source could include the control panel identification (ID) and the instrument ID. To detect an onsite relay status, the information source could include the building identification (ID) where the relay is located, the room ID (of the building), the cabinet ID (of the room), the relay bank ID (of the cabinet), and the relay ID (of the bank), etc. To detect a specific drawing, the information source could include the building ID (in which the drawing is stored), the room ID, and the drawing sheet where the system drawing is located.*
- *The information: Some information sources only show one parameter's status (e.g., relay only shows on/off). Some digital information source can show multiple channels of information. To obtain the correct information, the individual may need to navigate the instrument interface to obtain the desired information.*
- *Indication range: Some indicators are only calibrated to cover a portion of the full possible range of a parameter shown on the scale. The individual has to know the range in order to correctly interpret the information. For example, an out of bound indication cannot be interpreted as the parameter is in a steady state.*
- *Indication reliability: Some digital displays alternate display format (e.g., change font color and blinking fonts) to indicate the parameters are at an abnormal status.*

Indication availability and reliability

In the situations of a large scale of instrumentation failure (e.g., due to the loss of instrumentation power), many indications may not be available or not reliable. In this condition, assessing a parameter's value could be challenge because the operator needs to integrate multiple plant symptoms, available information, and considerations of indication reliability to reasoning to conclude the right parameter value (value range). The cognitive activities (reasoning to make a conclusion) are similar to the understanding macrocognitive function. For example, determining RPV water level in the loss of instrumentation power situation as in the Fukushima Daiichi event, the RPV water level has to be estimated by integrating decay heat, injection flow rate, RPV geometry, and leakage flow, etc. In this situation, determining the RPV water level became an understanding macrocognitive function instead of detecting macrocognitive function.

Ergonomics

The MCR crew constantly monitors a set of plant parameters important to plant operation during accidents. Examples for PWR include subcooling margin, RCS temperature and pressure, SGs' water levels and pressures, and pressurizer water level. During sever accident situation the RPV water level, core exit temperature, containment temperature and pressure, hydrogen concentration, containment inert status, electric power supply, and water supply, etc. are important to the decision makers. Examples of BWR important parameters include RPV water level and pressure, containment pressure and temperature, suppression pool water level and temperature, hydrogen concentration, electric power supply, and water supply, etc. If the instrument performs its designed functions, then the issue would mainly on whether the operator is checking

the correct instrument and whether there are ergonomic or other consideration that may affect the detection. Common procedure commands are:

- *check if the pressurizer pressure is greater than X psig*
- *check if a valve is open*
- *check of the pressurizer pressure is stable or increasing*

A common thing to the above three bullets are the values or statuses of the parameters of interest are directly indicated by indicators. There is no need to integrate different information (shown in other indicators) to conclude the values or statuses of the parameters. Even though the last bullet (check if the pressurizer pressure is stable or increasing) may require more cognitive efforts than the first two bullets, the operators are expected to be trained on detecting the trend of a parameters, therefore this type of activity is considered as detecting.

Redundancy

In some situations, a parameter may be simultaneously monitored by people at different locations using different instruments. For example, during a shutdown refueling, certain plant parameters has indicators at local location and in the main control room. The indication may or may not have an annunciator when the parameter value is outside of the set boundary. The probabilities of the local crew and the main control room crew detecting the parameter abnormality may be different. Either the local Crew or the MCR crew detect the abnormality in time would avoid an undesired consequence.

High Noise

In most situations, detecting an indication is instructed by procedure. This provides an explicit motivation for the operator to detect a piece of information. If detecting the information relies on operator's awareness instead of instructed by procedure, the success rate of detecting the piece of information strongly depends on the situation. For example, the unique dynamics of electricity fault in the H.B. Robinson fire event (March 28, 2011) closed a CCW flow control valve (FCV-626). This was not expected by the operators because the valve remained open in the simulator exercises of the similar scenarios. This was because the H.B. Robinson's simulator did not model to the level of details needed to replicate the dynamics of the event. In this event, the operator did not detect the valve closure until later in the scenario guided by procedure. In this event, hundreds alarms were triggered. This example shows difficulty in noticing a plant abnormality when the abnormality is not expected by the operator and the information (signal) is presented among many other information (noise). This situation only exist in ASP and SDP event analyses but not in base PRA (SPAR) because the event analyses of ASP and SDP are analyzing the occurred events but the Base PRA analysis is for a hypothetical event.

Scenario Dynamics

In certain situations, the indicator may display correct plant information but the information may not be the correct information to be used in procedure because reasons such as scenario dynamics and timing. An example is in the loss of coolant accidents (LOCA) the procedure asks for RCS temperature trend to determine if RCS having

sufficient (long term) cooling. If the operators arrives at the procedure step soon after the accumulator injected coolant into RCS, the RCS temperature is trending down because of the temporary accumulator injection rather than long term RCS cooling. Therefore, in this procedure context, even though the displayed RCS temperature is trending down (for a short period of time) but based on the scenario dynamics (accumulator was actuated earlier), in answering the procedure question, the operator should wait a little bit longer to provide the long term trend to follow the procedure.

Indicator Failure

In certain situations, indicator may fail to display correct value. The operator is trained not to rely on a single indication for information but to check other redundant or relevant indications for information. Typically there are redundant indications or other information available for the operator to conclude a failed indication. The operators are trained to check relevant indications for correct value or status. Therefore, a successful detecting cognitive function is to detect the "correct value (or status)" instead of the face value (or face status; as shown in a failed indicator). In other words, successful detecting macrocognitive function also include confirming the information is a valid information.

An indicator displays out-of-bound indications (e.g., above the upper bound or below the lower bound) may be informative depending on the diagnosis need. For example, the exact reading of an indicator is not available for an above the upper bound indication. However, it still provides the information that the parameter's value is above the upper bound setting of the indicator. This piece of information could be useful for understanding the plant problem. Other forms of instrumentation failure could include:

- *Using an off-calibrated tool to calibrate the instrument.*
- *The indicator operates outside of its operational condition. For example, water level measurement is sensitive to the water density of the sensing line. In an adverse environment condition, the sensing line water may be evaporated, boiling, or having significant density change due to change in surrounding temperature. In these situations, the indication is no long reliable.*

PIF considerations for Understanding

Correct understanding is the foundation for correct decisions. Having a correct understanding includes having a holistic picture of the situation for knowing the task priorities and potential conflicts among the concurrent tasks. Therefore, it includes having a mental model of the plant responses to assess the near term plant status (instead of current plant status). For example, operators may use currently available information to estimate the time to exceeding a plant threshold (e.g., time to exhaust of the essential batteries, and time to core uncover (as occurred in the Fukushima Daiichi event), and time to containment reaching to a high pressure, etc.).

Even though there are many procedures (e.g., alarm response procedures (ARP), abnormal operating procedures (AOP), emergency response procedures (EOP), and severe accident management guidelines (SAMG), etc.) available to assist operators to diagnose an abnormal event. Nevertheless, the procedures never be perfect. Human's judgement is needed to apply the procedure properly to understand the situation and to make correct decision (with the assistance of procedures). For example, in a PWR, soon after the accumulator actuation following a loss of coolant accident event, the RCS

temperature will decrease for a short period of time and then heat up again. The operator should know the RCS temperature trend asked in the loss of heat sink EOP emergency procedure is about if there is sufficient RCS heat removal capability. The accumulators only provide temporary RCS cooling. The operators have to understand that the RCS does not have enough cooling to follow the procedure correctly.

In rare situations, the operators may determine that the procedure is leading to a place the operator does not want to go, i.e., the operator's mental model of the event differs from the procedure. In the EOP space, the U.S. plants typically require two SROs agree to deviate from procedure instructions. This is to illustrate a point that in applying procedures, the operators also independently apply their mental model to understand the event because the operators has more plant operation history information and observer more plant symptoms than asked by procedures. The consistency between the operator's mental model and the procedure instruction is an important factor affecting operator's confidence in following the procedure instruction. In other words, this affect the likelihood operator decide to deviate from procedure instruction. Therefore, HRA analysts should not heuristically conclude that the diagnosis is straightforward because there is a procedure for the event. The event details and the procedure instructions may not consistent. That poses a challenge for the operator to implement the procedure.

PIF consideration for decision-making

An NPP has a large set of procedures that provide response plans for a wide range of incidents and accidents. The AOPs and EOPs typically provide clear step by step instruction as response plans for situations. For example, E-3 specifies that the response plan for isolating the broken SG(s) includes adjusting the ruptured SG(s) PORV controller setpoints; checking that the ruptured SG(s) PORVs are closed; closing steam supply valves from the ruptured SG(s) to turbine-driven AFW pumps; verifying blowdown isolation valves from the ruptured SG(s) are closed; and closing the ruptured SG(s) main steamline isolation and bypass valves. After completing these actions, E-3 guides the operator to check the ruptured SG(s) water level to ensure the actions are properly performed.

US operators are required and are incentivized to adhere to procedure instructions. Therefore, except for when there are strong justifications to the contrary, the operators are expected to follow the response plan specified in procedures. This expectation does not mean that operators would implement procedure exactly as instructed by the procedure. The operator has certain flexibility in implementing procedures. For example, if the procedure specified component is not an option in the scenario, the operator has to decide the alternative to achieve the same function. In some situations, the operators may decide to deviate from the procedure instructions. For example, in implementing procedures the operators are constantly maintaining awareness of the scenario progression and looking ahead in the procedures to maintain awareness of the procedural path. If the operator senses that the procedure is guiding towards a destination that inconsistent with the operators' perception of the situation or that is in a direction that the operator is hesitant to go (e.g., the decision has high economic consequences), the operator may deviate from the response planning as specified in the procedure.

In the situations where there is no appropriate procedures to provide a response plan, the operator has to perform the task based on knowledge. In such situations, the response plan is less comprehensive and more prone to error than if there is a suitable procedure available.

PIF considerations for Action

For nuclear power plants operations, most events have corresponding procedures that provide pre-planned action instructions. In rare situations, there may not be pre-planned responding instructions readily available. In this situation, on scene development of the less thorough action scripts may be needed, e.g., implementing a creative alignment to remove decay heat when the pre-planned options are not available. The following are some considerations related to performing actions:

- *Action types: Actions could be as simple as turning a switch in the control room, or using the mouse, rolling ball, keyboard, and touch screen to navigate through the computer user interface to select the desired actions, or opening a few valves to align systems and components.*
- *Action duration: Actions can be short such as pushing a button, or long such as follow through an event procedure (e.g., SGTR procedure), or slowly depressurize RPV with monitor-and-control type of actions (e.g., in a cooldown rate not exceeding 100 °F/hr), or setting up a potable pump to inject coolant, etc.*
- *Work environment: Actions could be performed within an air-conditioned and well lighted workplace (e.g., main control room) or on site with poor lighting, ergonomically challenging, and harsh environment (e.g., high temperature, high humidity, and high radiation level, etc.). The work environment not only includes the environment of the work place but also the travel path to the work place. Harsh environment in the travel path and work place could prevent the actions from been executed. Work in high radiation areas would have time limitation on how long an individual can stay in the work area. Entering certain areas of the plant requires wearing protective cloth. This may affect human performance.*
- *Special tool: Some actions requires special tool to perform. Actions such as using portable pumps to inject into RCS or RPV may require the use of a ranch to open a blind flange to connect to the injection hose. Towing vehicles may be needed to move a portable pump or generator.*
- *Evaluate action effectiveness: Actions on component typically can obtain immediate feedback to confirm that the action is successfully performed. For example, changing a valve position by turning the valve's control switch, the valve's position indication light would switch color to confirm the action completion. Change in flow rate indication could confirm that the action was successfully performed. Some actions' effects may take longer to appear. For example, injecting into a boiling steam generator would see the SG water level decrease first then increase later, inject into an overheated core may take a while to see the RPV temperature trending down, and taking a while to detect an RPV increasing water level after injecting water into an uncovered core.*
- *Recover effects from incorrect actions: Some actions if performed incorrectly can be recovered immediately. Some require significant efforts to undo the effects of the error actions. Some may require considerable time and effort to identify the correct actions to correct the problem. This could delay event recovery or complicate the efforts in handling the event. Examples are:*
    - *Turning a valve into a wrong position typically can be corrected by turning again to the right position.*

- *Turning a control to a wrong position could mis-align the system. Realigning a system could take some efforts.*
- *Shedding dc load is a time sensitive action in a SBO or an ELAP event. This task could include switching open more than 100 breakers in various locations inside the reactor and turbine buildings at a condition poor lighting and a sense of urgency to complete the task to prolong dc power. If the individual mistakenly switch open a breaker which should not be open without noticing the mistake, it may take a few hours to remove the mistake after perceiving the abnormal status.*

In the loss of main and auxiliary feedwater event at the Davis-Beese plant in June 9, 1985, the secondary side operator incorrectly switched the Steam Feedwater Rupture Control System (SFRCS) to low pressure mode instead of the intended low level mode. The incorrect actions shut off the auxiliary feedwater (AFW) system. After noticed both AFW pumps tripped, "the shift supervisor quickly determined that the valves in the AFWS were improperly aligned. He reset the SFRCS, tripped on low level, and corrected the secondary operator's error one minute after it occurred" (NUREG-1154). However, in this event, two AFW isolation valves failed to open automatically after the SFRCS was reset to low level trip. The operators tried to open the valves from control room without success. The valves had to be reopened on site. The Davis-Beess event is an example that significant amount of efforts may be needed to recover from a human error.

- *Coordinated actions: Actions to achieve the objectives could be performed by multiple individuals to coordinate things such as action timing and situation-based action specifics, etc. These individuals may be located at different locations that require communication means for the coordination.*
- *Manpower and skillset: after Fukushima Daiichi event, the U.S. plants procured portable equipment to mitigate the hypothetical extended loss of heat sink (ELAP) and the loss of ultimate heat sink (LUHS) event. The mitigating strategies are referred as FLEX strategies. Implementing the strategies requires team efforts to clean debris in the equipment transportation route and staging locations, moving the portable equipment to the staging locations, and setup and operator the portable equipment, etc. Performing the mitigation strategies not only require sufficient manpower but also the need skill to operate the equipment. In an extreme event that the site accessibility is limited, the manpower and skillset could be a limiting factor for success actions.*

6 Development of application-specific quantification model

The Basic Quantification Structure provides a full set of CFMs and a comprehensive list of PIFs. In theory, it can be used to perform HEP quantification for any HRA application. Yet, assessing the full set of CFMs and all the PIFs can be very time-consuming. Moreover, the descriptions of the CFMs and PIFs may not fit to a specific application. Lastly, the HEP of a CFM is determined by the status of its associated PIFs, the numerous combinations of many PIFs can make HEP estimation difficult if not impossible. Therefore, when using IDHEAS-G for HEP quantification, we recommend that an application-specific quantification model should be developed from the Basic Quantification Structure. A quantification model should include the following:

1) The assumptions for the specific application; they are the basis for developing the quantification model and they specify the scope that the model applies.
2) A concise set of CFMs that represent the full range of cognitive activities for tasks in the specific application;
3) A set of PIFs that represent the application-specific context
4) Selection of a way to quantify the effects of PIFs on CFMs
5) The HEP distribution for the CFMs at any combination of PIF status.

This chapter provides guidance and two examples on developing application-specific quantification models. One example is NPP internal at-power application, the other is for NPP ex-control room actions in severe accidents (e.g., use of FLEX equipment).

6.1 Identify the scope of the application-specific model

The first step to develop an application-specific model is to understand the context of human actions in the application and make general assumptions about the application. This is done by reviewing the nature of the system, tasks, personnel performing the tasks, and the high-level PIFs in the application. The assumptions are the basis for selecting subsets of CFMs and PIFs. Below are some guidance questions:

Nature of the system:

- Is the system a human supervisory system (human in control of automated subsystems), non-automated system, or a passive system (to which human only take monitoring roles)?
- Are the scenarios for normal, emergency, or accident operation?
- What are the operational modes of the systems?

Nature of the tasks:

- Are the tasks proceduralized?
- Are there command and controls?
- How do the five macrocognitive functions involve in the tasks?
- Where do the tasks typically performed?

Personnel performing the tasks:

- Who are the primary personnel performing the main tasks?

- Are the primary personnel a well-trained crew or a group of untrained person?

PIFs:

- Work environment
- Work process (e.g., command and control, authorization, infrastructure for coordination and cooperation)
- Organizational factors,
- Stress and pressure,
- Fatigue and fitness-for-duty.
- Human-system interface (HSI) and tools
- Procedures,
- Training

The first example is for modeling NPP internal at-power events. The following assumptions are made for the quantification model of IDHEAS internal, at-power application:

- The system modeled is a NPP under the at-power operation mode.
- The PRA scenarios modeled are Level-1, internal, abnormal or emergency events
- The tasks mainly involve the macrocognitve functions of Detection, Understanding, and Execution. Even Decision-making is limited to choose and implement strategies in procedures. Teamwork is achieved through control room crew structure.
- Well-trained crew perform the critical tasks in the main control room.
- Work environment is generally good for CR operation in internal events
- CR crew meets fitness-for-duty requirements so fatigue, stress, and pressure should not be a concern for operator performance.
- HSI and procedures have been thoroughly tested and validated, and operators are well trained with them.

The second example is for modeling ex-control actions in accident scenarios. The assumptions include but not limited to the following:

- The systems being modeled include NPP reactors, contaminate, spent-fuel pool, and any other safety-critical systems
- Tasks involves all the macrocognitive functions. In particular, decision-making and teamwork can be challenging; Innovate solutions may be used.
- Personnel included trained crew as well as untrained individuals; staffing may be inadequate.
- Procedures, guidelines, and instructions may not be available or applicable.
- Work environment can be harsh
- Work site can be anywhere outside the main control room. Some actions may be performed un-sheltered.
- HSI, equipment, and tools may be degraded or not work.
- Stress, pressure, fitness-for-duty, and fatigue can become significant

The first set of assumptions should allow a quantification model with only a small subset of the CFMs and PIFs. In contrary, the second set of assumptions leaves little room for

eliminating non-applicable CFMs or non-significant PIFs. A special case for the second example is that a quantification model is needed to analyze the reliability of executing human actions in FLEX strategies given that the decision for implementing the actions is already made. In this case, the assumption about the tasks is that only the Action execution and Teamwork macrocognitive functions need to be considered.

6.2 Selection of the CFMs

Depending on the HRA applications, the CFMs for the given application can be derived from the Basic Quantification Structure in different ways:

- Elimination: Some CFMs may not be applicable therefore they can be eliminated. For example, the NPP internal at-power application assumes that decision-making is limited to choosing and implementing the strategies specified in procedures; many CFMs for the Decision-making macrocognitve function can be eliminated. Caution for elimination is that some eliminated CFMs could appear in an unexpected event scenario and the elimination may lead to gaps in CFM representation and result in underestimation of HEPs.
- Merge: The CFMs of some proximate causes may not be behaviorally distinguishable, or the effects of the PIFs on these CFMs are indistinguishable. Therefore, the CFMs can be groups into a single one for HEP estimation. In other cases, the HRA application may only require some screening or scoping quantification of HFEs and do not need a more accurate HEP estimation, then the CFMs can be grouped together according to the PCs or macrocognitve functions for quick assessment. Caution for merging CFMs is that the merged high-level CFMs may become insensitive to differences in tasks.
- Split: An HRA application may involve in modeling a very specific type of human actions, then it may worth to split one CFM to several more detailed ways that the PC is performed incorrectly. Caution for splitting CFMs is that information about task context or PIF status may get lost with too detailed CFMs.
- Refinement: The description or definition for the CFMs in the Basic Quantification Structure are generic and may not be applicable to the given HRA application or difficult to interpret them in a specific domain. They can be refined with more application-specific description. Caution in refinement is that a CFM meant to cover multiple ways leading to a PC now only cover a subset of the ways. This may also result in underestimation of HEPs.

Overall, the basic principles for develop an application-specific CFM set are the same as we identify CFMs for the Basic Quantification Structure: CFMs should form a complete representation of the tasks and CFMs should be behaviorally observable. Table 6-1 presents the CFM set developed for internal at-power application.

Table 6-1 Selection of CFMs in IDHEAS Internal At-Power Application

Cognitive process	CFMs in Basic Quantification Structure	CFMs for internal at-power application
D1- Initiate detection - Establish mental model and criteria	D1-1 Detection not initiated (e.g., Skip steps of procedures for detection, forgot to check information, no instruction for detection)	

for information to be acquired	D1-2 Wrong detection criteria used D1-3 Fail to prioritize information to be detected	
D2 - Identify and assess equipment needed	D2-1 Fail to prepare the right measurement equipment / detection tools, or inspection systems (equipment incorrectly identified; unable to operate equipment,; incorrect calibration of the equipment)	
D3 – Identify and attended to sources of information	D3-1 Fail to access the source of information (fail to access, view, or measure partial or all sources, motor failure in probe movement to sub-areas for detection) D3-2 Wrong source attended	Wrong source attended
D4- Perceive information	D4-1 Key alarm not attended to	Key alarm not attended to
	D4-2 Fail to recognize that primary cue is not available or misleading	Data misleading
	D4-3 Cues (abnormals) not perceived	
	D4-4 Cues misperceived (information Incorrectly perceived, fail to perceive weak signals, reading errors) D4-5 Fail to monitor status (e.g., Information or parameters not monitored at proper frequency or for an adequate period of time, fail to monitor all the key parameters)	Critical information misperceive d
D5- Recognize, verify, and confirm information acquired	D5-1 Incorrectly interpret, organize or classify information	Covered by “Critical information misperceive d”
D6- Communicate the acquired information	D6-1 Detected cues not retained or incorrectly retained (mark wrong items, wrong recording, wrong data entry) D6-2 Cues not communicated or miscommunicated	Not applicable
U1 - Assess/select data	U1-1 Incomplete data selected (e.g., critical data dismissed, critical data omitted) U1-2 Incorrect or inappropriate data selected (e.g., fail to recognize the boundary conditions of data, not recognize information age)	critical data dismissed
U-2 Select / adapt / develop the mental model	U2-1 Incorrect mental model selected U2-3 Fail to recognize mismatched procedures (e.g., fail to adapt procedures)	
U-3 Integrate data with mental model to generate understanding (situation	U3-1 Incorrectly assess situation (e.g., Situational awareness not maintained, Incorrectly predict system evolution or upcoming events)	

awareness, diagnosis, resolving conflicts))	U3-2 Fail to or Incorrectly diagnose problems (e.g, Conflicts in data not resolved) U3- 3 Fail to use guidance outside main procedure steps (e.g., fold-out pages) in diagnosing	
U-4 Verify and revise the understanding	U4-1 Premature termination of data collection (e.g., Not seek additional data to reconcile gaps, discrepancies, or conflicts, Not revise the outcomes based on new data, mental models, or view points) U4-2 Individual's biased or incomplete understanding accepted by the team (e.g., assessment or diagnosis not verified or confirmed by the team, lack of confirmation and verification of the results in the work process) U4-3 Fail to generate coherent team understanding	Premature termination of data collection
U-5 Communicate the outcome with other parties	U5-1 Outcomes of Understanding miscommunicated or inadequate communication	
Cognitive process	**Cognitive Failure Mode**	
DM1 – Manage the goal	DM1 – 1 Incorrect goal selected DM1 – 2 Incorrect prioritization of goals	
DM2 – Select or develop a decision model to meet the decision goals and criteria	DM2 – 1 Incorrect decision model (e.g, heuristic is used, no decision-model meets the goals) DM2 – 2 Incorrect decision criteria	
DM3 – Acquire / select information to be used for DM	DM3 – 1 Critical information not selected or only partially selected (e.g., under-sampling information) DM3 – 2 Selected information is not appropriate (e.g., out dated, not applicable for the situation) DM-3 Misinterpret or misuse selected information	
DM4 - Make decision (judgment, strategies, plans)	DM4 – 1 Misinterpret procedure DM4 – 2 Choose inappropriate strategy in procedures DM4 – 3 Incorrect judgment DM4 – 4 Incorrect or inadequate planning or developing strategies / solutions (Plan wrong or infeasible responses, Plan the right response actions at wrong times, Not plan configuration changes when needed, Plan wrong or infeasible configuration changes) DM4-5 Incorrectly decide to interfere with automated safety systems (i.e., error of commission) that has adverse impact on safety	Misinterpret procedure Choose inappropriate strategy
DM5 - Simulate / evaluate the decision / plan	DM5 – 1 Fail to or unable to simulate or evaluate the decision DM5 – 2 Incorrectly simulate or evaluate the decision	

DM6 - Communicate and authorize the decision	DM6 – 1 Decision not properly communicated DM6 – 2 Decision not authorized or delayed authorized (e.g., unable to authorize the decision due to ambiguity or problems in authority)	
E1–Assess action plan	E1-1 Incorrectly assess or interpret the action plan (e.g., errors in personnel allocation, equipment / tool preparation, or coordination) E1-2 Wrong action criteria selected E1-3 Incorrect decide to manipulate safety systems outside the action plan (e.g., error of commission)	
E2 - Develop / modify action scripts	E2-1 Fail to modify or develop action scripts as needed	
E3– Synchronize, supervise, and coordinate action implementation	E3-1 Delayed implementation E3-2 Action not initiated (e.g., Fail to coordinate actions, Not perform the plant status checking required for initiating actions, Failed command & control)	Delayed implementation Action not initiated
E4 - Implement action scripts	E4-1 Fail to follow procedures (e.g., Skip steps in procedures, steps performed in wrong orders or at wrong timing, action criteria not followed) E4-2 Fail to execute skill-of-craft actions E-3 Fail to execute simple action E4-4 Fail to execute complex action (Execute all the steps of a complex action in wrong timing or sequence, Execute actions that do not meet the entry conditions, Not or mis-coordinate execution of complex actions among team members) E4-5 Fail to execute long-lasting actions	Skip steps in procedures Fail to execute simple action Fail to execute complex action
E5 - Verify and adjust actions	E5-1 Fail to adjust action by monitoring, measuring, and assessing outcomes E5-2 Fail to complete the entire action plan (e.g., omit steps after the action criteria are met) E5-3 Fail to record, report or communicate action status or outcomes	

6.3 PIFs Selection

Selection of PIFs for an application-specific model from the Basic Quantification Structure first depends on how to quantify PIFs, i.e., modeling the effect of multiple PIFs on the HEP of a CFM. PIFs can be quantified in two ways:

1) *Holistic decision-tree estimation* – The contribution of all the PIFs to the HEP of a CFM are considered together without specifying individual contributions and interactive effect among the PIFs; a CFM may have multiple HEP vales, each corresponding one combination of PIF status. For example, if a CFM has 3 relevant PIFs, and each PIF has two status (e.g., normal vs. poor), then the CFM can have 9 HEP values each corresponding to one of the 3x3 PIF combination. Practically, holistic estimation can only be manageable with a limited number of PIFs. An example of the holistic estimation is the use of decision-tree to represent a few the most relevant PIFs for every CFM. Another example is to model a limited number of PIF combinations that are typical for the application

2) *Individual estimation* – The contribution of every PIF to the HEP of a CFM is individually estimated, then the effect of all the PIFs on the HEP are combined according to some pre-specified rules. This approach allows to consider many PIFs together. The limitation is the HEP highly depends on how the interaction among the PIFs is modeled. For example, some HRA methods assume that the combined effect of PIFs are multiplicative; while some other methods assume that the combined effect is the sum of individual contributions. Appendix E provides information synthesized from cognitive literature about PIF interaction.

Like the CFMs, PIFs for an application-specific quantification model can be derived from the Basic Quantification Structure in the following ways:

- Elimination: Some PIFs may not be applicable therefore they can be eliminated. If the model uses holistic estimation, then elimination may be necessary for those that are not applicable those that are known for their insignificant contribution to the CFM. Elimination should start by reviewing the assumptions of application. For example, one assumption for NPP internal at-power application is that human actions are performed by well-trained crew in control rooms. Thus most environmental factors 9except smoking from internal fires) are eliminated Caution for elimination is that some eliminated PIFs could appear in an unexpected event scenario and the elimination may lead to missing an important error causal factor in the event analysis and underestimation of the HEP.
- Merge: The effect of several PIFs may not be distinguishable therefore they can be grouped into one category for consideration. Also, merging detailed PIFs like those in the Basic Quantification Structure is used as a trade-off between model complexity and sensitivity. Caution is that the merged high-level PIFs may become insensitive to differences in tasks and lead to subjectivity in HRA analysts' assessment of the PIFs, resulting in analyst-to-analyst variability in HEP estimation.
- Refinement: The description or definition for the PIFs in the Basic Quantification Structure are generic and may not be applicable to the given HRA application or difficult to interpret them in a specific domain. They can be refined with more application-specific description. Caution is that the cognitive mechanisms underlying the PIFs should be carefully reviewed to ensure that the mechanisms are captured with the refined PIFs.
- New PIFs: The comprehensive list of PIFs in the Basic Quantification Structure represents our state-of-knowledge PIFs. New PIFs may become significant for unknown or unknown-unknown scenarios, unknown applications, or development

of new technologies. Whenever a new PIF is identified, they should be assessed against the cognitive mechanisms for their potential impact on the CFMs.

Table 6-2 shows an example of PIF selection in the quantification model of IDHEAS internal at-power application. Only the PIFs for one CFM, "Information misperceived" are presented. The model uses holistic decision-tree estimation, so only 3-4 most relevant PIFs are considered for the CFMs. The selected PIFs form a decision-tree for a CFM, with each branch point representing one PIF. Table 6-2 indicate that many PIFs in the Basic Quantification Structure were eliminated or merged. Essentially, three CFMs are left for the CFM in internal at-power application: HSI, Workload, and Training. A decision-tree is thus built with each branching point representing one of the PIFs. The cognitive mechanisms associated with every CFMs were examined to ensure that the eliminated PIFs and unrepresented CFMs were justified within the assumed scope of NPP internal at-power application.

Table 6-2 Selection of PIFs for the CFM "Critical information mis-perceived" in IDHEAS Internal At-Power Application

PIFs in Basic Quantification Structure	**PIFs in the quantification model of IDHEAS Internal At-Power Application**
Information reliability - Sensors or indicators may be unreliable (e.g., damaged, degradation, false alarms in design, out-of-range, inherently unreliable sources, problems in communication, or flaw in system state indication)	
Information signal is weak or masked (visually or aurally)	
Primary sources of information are not available while secondary sources of information are not reliable, perceivable, or understandable	(Addressed by another CFM)
Detection criteria are complex (e.g., multiple criteria to be met or in complex logic)	Training
Criteria are not applicable to the information	
Criteria are ambiguous	
Unfamiliar scenario	
Intermingled multitasking	Workload
Frequent or persistent interruption/distraction	Workload
Unpredictable system dynamics	
Cognitive complexity in detection – Information demands may exceed the individual's working memory capacity: o Concurrently monitor 3 or more than 3 non-related developing situations. o Concurrently monitor 7 or more parameters Mentally retain multiple pieces (> 7) of information	

Time pressure and other stresses	Workload
Mental fatigue o Long working hours under stress or in harsh environment Sustained high-demanding cognitive activities (e.g., information changes over time and requires sustained attention to monitor or check at a certain frequency for a long period of time.	
CLARITY: Confusion of indications or un-intuitive indications. The indication or label can be interpreted differently for reasons such as imprecise in axis labeling in an X-Y plot	HSI
The process needed to obtain the information, e.g., the information of interest has to be determined based on the status of other pieces of information. o The number of information needs to be checked to determine the information of interest: Involve 2 or more than 2 types of logic operators (e.g., AND, OR, NOT, and NOR.)	
SALIENCE: The information has similar appearance with surrounding information o The information to be detected is buried in a large amount of potentially relevant information. o The information cannot be easily identified because the environment causing visual or auditory camouflage. o The information has human factors issues (e.g., font is too small and located too far and poor lighting, misuse of colors, etc.) Visibility of information is low due to environmental factors	HSI
PROLONGED ATTENTION: Information changes over time and requires sustained attention (> 10 minutes). o Determining a parameter trend during unstable system status that required continuous attention for more than 10 minutes. For example, determining the RPV temperature trend in the situations of water just injected into the RPV. It would take some time to see the stable temperature trend. Monitoring a slow-response-system's behavior without clear time window to conclude the system response/behavior.	
Training: Inadequate training on urgency / criticality of key information	Training

6.4 Guidance for HEP estimation in the quantification model

A quantification model should be an off-the-shelf product with a set of CFMs, the PIFs for every CFM, and HEPs for given PIF combinations in the model. If the holistic estimation is used, the model shall provide the HEP distribution for every PIF combination represented in the decision-tree or every selected failure scenarios. For individual estimation, the model shall provide rules for calculating and combining the effects of individual PIFs.

Human error Probability (HEP) can be interpreted as the number of errors divided by the number of demands for the response for the event in consideration. In the IDHEAS quantification model, each DT path represent one type of failure scenario characterized by the status of the PIFs. The HEP for a given DT path is the likelihood of the CFM for the given status of the PIFs. Three common methods have been used in quantifying event probabilities in PRA, as noted in the NRC's guidance for treatment of uncertainties in risk-informed decision-making (NUREG-1855):

- Frequentist Approach defines the probability of a random event as the long-term fraction of times that the event would occur in a large number of trials.
- Bayesian Approach characterizes what is known about the parameter in terms of a probability distribution that measures the current state of belief in the possible values of the parameter.
- Expert Judgment. The expert judgment approach relies on the knowledge of experts in the specific technical field who arrive at "best estimates" of the distribution of the probability of a parameter or basic event. This approach is typically used when detailed analyses or evidence concerning the event represented by a basic event are very limited or unavailable. Such a situation is usual in studying rare events. Ideally, this approach provides a mathematical probability distribution with values of a central tendency of the distribution (viz., the mean) and of the dispersion of the distribution, such as the 5th and 95th percentiles. · The distribution represents the expert or "best available" knowledge about the probability of the parameter or basic event. The process of obtaining these estimates typically is called "expert judgment elicitation," or simply "expert judgment" or "expert elicitation."

To estimate the HEPs for various combinations of PIFs pertinent to a CFM, the quantification model developers need to first assess the available data about human error rates or error probability for the cognitive tasks. The ideal situation is that the available data allows for the frequentist approach. When the data is sparse, expert judgment is needed to estimate the HEPs. For eliciting expert judgment, we recommend the use of the Senior Seismic Hazard Analysis Committee (SSHAC) Method (NUREG/CR-6372, *Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and the Use of Experts*) because this method is recommended as the method to formally use expert judgment in risk-informed decision-making [**ref, the expert judgment SRM and the NRC's position NUREG to be published in 2017].

SSHAC defines a formal, structured, interactive process for conducting expert judgment on complex technical issues. The outcome represents the center, body, and range of the

knowledge / interpretations / judgment by the informed technical community. SSHAC embeds the following principles:

- Structured – A structured, formal expert panel and the structured process facilitates elicitation and minimizes biases.
- Breadth of State-of-Knowledge – The experts (as representatives of the informed technical community) evaluate all the available evidence (e.g., numeric data, models, theories, and scientifically accountable positions) to make their judgment.
- Independence – Judgment is based on knowledge and individuals' expertise; it is not influenced by the organizations that the experts represent.
- Interaction – The process of evaluation, elicitation, and integration is achieved through interaction among the experts with an emphasis on addressing uncertainties in the problems being judged.
- Integration - The process emphasizes integration (rather than consensus) of individuals' interpretations or judgment.

[Note: should we add a paragraph overviewing SSHAC process or just point to SSHAC guidance document?]

The quantification model in IDHEAS internal at-power application used the SSHAC process to refine the CFMs and decision-trees as well as estimate the HEP distributions of DT paths for every CFM. Each HEP distribution includes the body, range, and central tendency (i.e., the mean HEP). The expert panel includes NPP operational personnel, PRA/HRA experts, and human factors and cognitive psychology scientists. The rigorous SSHAC process provide reasonable assurance that the estimated results represent the distribution of the informed PRA and NPP communities.

Appendix F provides an example of using available data from cognitive literature and several human error database to infer a set of rules calculating and combining the effects of individual PIFs, and estimating the parameters to calculate the HEP for any combination of the PIFs. This example demonstrates a way to estimate the HEP for situations where the scenarios in the application scope vary widely and have too many uncertainty factors to limit the CFMs and PIFs to a reasonable small set, or where the application is for a rarely practiced work domain and little experience has been accumulated to use expert judgment of HEPs.

[Note: This example is not included per SC recommendation on 10/22/2016. Discuss at the 3/22/2016 SC meeting whether this example or the details of the approach should be included in this report.]

In summary, this chapter provides high-level guidance on developing application-specific quantification models from the Basic Quantification Structure. An off-the-shelf quantification model includes a set pf CFMs, the PIFs for the CFMs, the rules to calculate and combine the effects of individual PIFs, and the HEP distribution for PIF combinations modeled. In order for a model being practically useful, trade-off has to be made when selecting a subset of CFMs and PIFs.

7 Integrative analysis – HFE Dependency analysis and Uncertainty documentation

This section provides guidance on integration of the HRA for individual HFEs into the PRA. The components of model integration addressed in this chapter include: HFE dependency analysis and uncertainty documentation. The fundamentals of each of these steps in the HRA process are not unique to IDHEAS. The methods described in this section are based on current state-of-practice with some insights from the cognitive basis of IDHEAS-G This chapter is an area for future research.

7.1 Dependency Analysis

7.1.1 Conventional approach

The conventional approach to model dependence and dependence effects on HEP is by answering the following four questions to determine the dependence level between two consecutive HFEs of the same event sequence:

- Are the two tasks performed by same person or the same group of people?
- Are the two tasks performed at the same location?
- Are the two tasks performed close to each other in time?
- Are new cue(s) are available to perform the second task?

The above questions are good for screening to identify the tasks that tasks dependency may exists. For example, the dependences between pre-initiator tasks such as valves or switches left in a wrong position, calibration errors, or use of incorrect fuel, lubricant or additives are modeled in PRA (Vaurio, 2001). These activities could be implemented by the same person (people) with the same cue(s) (e.g., the same procedure or using the same calibration equipment). The dependences between post-initiator tasks, the PRA's typical modeling philosophy is the failure of an HFE could affect the HEP of the immediate downstream HFE of the same event sequence. Based on the answers to the above four questions, the dependency level could be one of the following five classes:

- zero dependence (ZD)
- low dependence (LD)
- moderate dependence (MD)
- high dependence (HD)
- complete dependence (CD)

The dependence level could change the second HFE's HEP (from the independent HEP to dependent HEP).

The above task dependency modeling is a simplified surrogate approach. It does not specify the cognitive mechanisms causing the dependence at the level that performance improvement to reduce the dependence can be practically implement. "A more realistic and defendable approach to the treatment of dependency between HFEs would clearly be to base it on consideration of the underlying human failure mechanisms in a manner analogous to the way in which common cause failures are addressed." (Parry, 2010)

The identification and effects of task dependence is strongly depends on the HRA methods. This is because each HRA method has the unique set of factors considered to calculate the independent HEPs. The dependence effects (to calculate the dependent HEPs) is to cover the effects not considered for the independent HEP calculation. Therefore, follow the guidance of the HRA method in use to specify the task dependence.

7.1.2 State-of-practice on HFE dependency

The analysis of multiple HFEs in accident sequences or cut sets is important because risk metrics such as CDF can be significantly underestimated if potential dependencies are not considered in determining the HEPs. The ASME/ANS PRA Standard [1] requires that multiple human actions in the same accident sequence or cut set be identified, an assessment of the degree of dependency performed, and a joint human error probability be calculated. For HRA, it is important to not only identify failure HFEs in the sequence, as would be the case in a review of the cut sets, but also to review successful operator actions that occur in the same sequence. The success paths would be identified through a review of the event trees and should be noted in the HFE definition. Where it is found that combinations of operator actions' HEPs are unduly multiplied in the cut sets (i.e., it appears that potential dependencies were not addressed), the appropriate level of dependency among the HEPs is to be assessed. Consistent with the ASME/ANS Standard, influences of success or failure on parallel and subsequent human actions and system performance should include the following:

- The time required to complete all actions in relation to the time available to perform the actions
- The availability of resources (e.g., crew members and other plant personnel to support the performance of ex-CR actions)
- Factors that could lead to dependence (e.g., common instrumentation or procedures, an inappropriate understanding or mindset as reflected by the failure of a preceding HFE, and increased stress; spatial and environmental dependencies should also be considered for external events)

The first two bullets above can be accounted for explicitly through construction of the basic integrated timeline in IDHEAS and comparing the necessary staff against those available. The third point, however, is more ambiguous, and discusses generically "factors that could lead to dependence."

We reviewed the dependency models used in existing HRA methods and literature on HRA dependency. Most of the methods use the quantitative dependency model proposed in THERP [2], with some slight modifications. NUREG-1792 "HRA Good Practices" [3] provides general guidance on treating dependencies, but also generally follows the THERP approach. NUREG-1792 [3] describes dependency as follows:

> 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 conditional 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 combined probabilities that are overly optimistic 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.

Among the methods, the dependency model in the Fire HRA Guidelines described in NUREG-1921 [4] represents the state-of-practice in the US NRC and EPRI based methods. Using THERP as a basis and consistent with ASME/ANS PRA Standard, the current state-of-practice, as described in section 7.3.1, examines a pre-defined set of factors likely to lead to dependency and then assigns a level of dependence based on the aggregated effect of these factors. While we have identified several limitations in the existing approaches to addressing dependency and the IDHEAS methodology has the potential to elucidate the dependency mechanisms because it allows human events to be analyzed while considering the underlying cognitive processes and the causal relationships (see further discussion in Section 8.3), this part of the IDHEAS methodology has not yet been developed. Thus, the treatment of dependency between HFEs in the present IDHEAS method uses the state-of-practice presented in NUREG-1921 [4]. Section 7.3.1 presents the adopted model.

7.1.2.1 Dependency Model

This section describes modeling dependencies among post-initiator HFEs. In general, the process of dependency analysis has four parts: understanding the PRA scenario and identifying those HFEs that are potentially dependent from a scenario point of view, then assessing which factors are present, establishing the level, and applying the equations or rules to adjust the HEP of the event. When a combination of HFEs is identified, a level of dependency can be assigned using the approach shown in Figure 7-1 and the THERP dependency equations shown in Table 7-1. Using the dependency rules below and following the appropriate branches through the table provides the dependency level for the second HFE. Table 7.1 translates the level of dependency into the conditional probability of the second HFE given that the first HFE has failed.

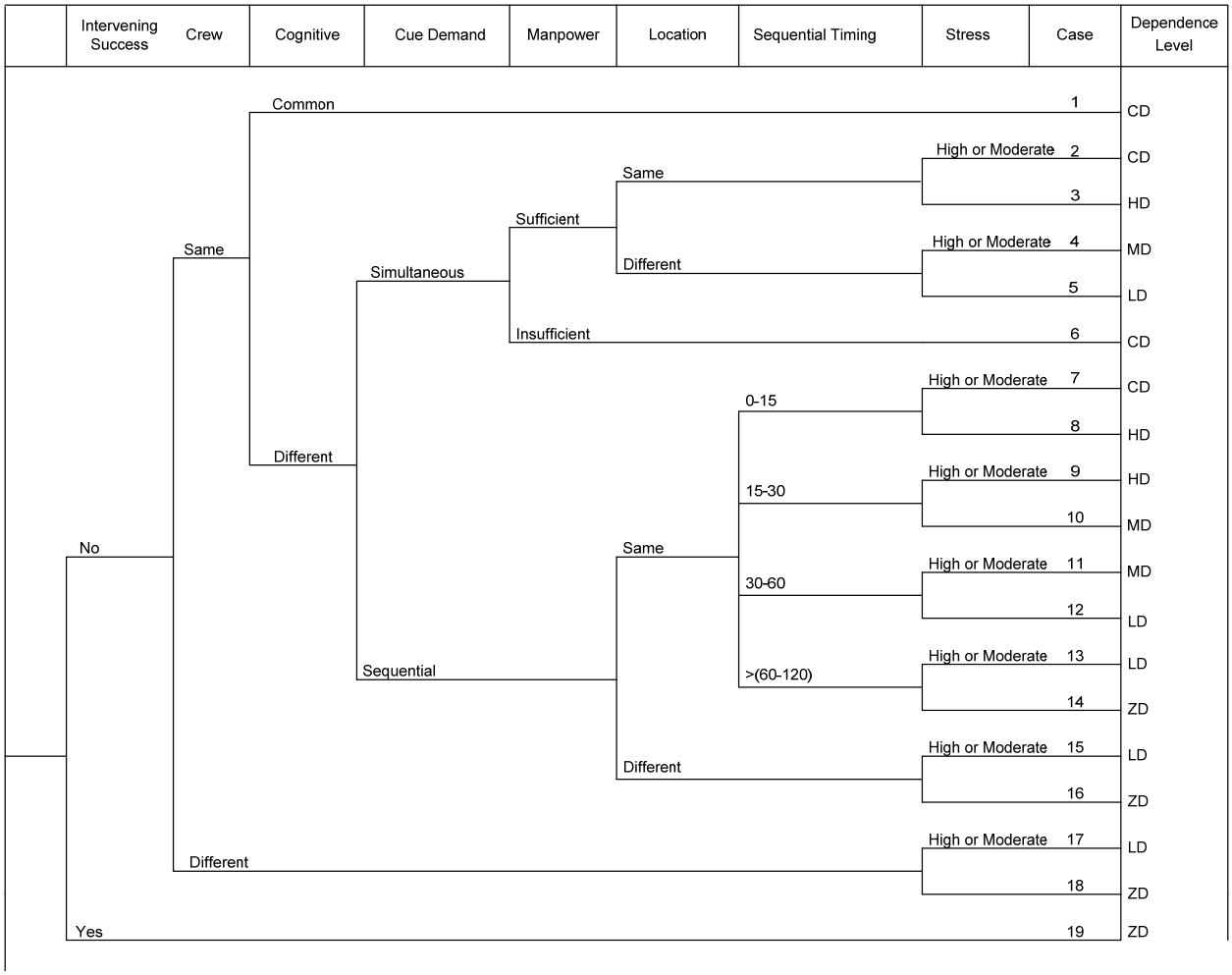


Figure 7-1. Diagram of dependency levels. CD – completely dependent, HD – highly dependent, MD – moderately dependent, LD – low dependent, ZD – Not dependent.

7.1.2.2 Dependency rules for post-initiator HFEs

The following elements are evaluated in the dependency analysis:

- **Intervening Success.** In accordance with THERP [2], an HFE is independent of an immediately preceding success. Therefore, if a successful action can be identified between the two HFEs, the two HFEs are considered independent.
- **Crew**. If the time between the cues for the required actions exceeds the length of a shift (typically 12 hours), the actions are to be performed by a different crew. In this case, the "No" branch on the "Crew" decision node is selected. The different crew can be considered independent because the shift change will involve a complete reevaluation of the plant status, so ZD can be assigned for low stress situations (Branch 18). For elevated stress such as a fire, LD is assigned. If the time between the cues is less than the length of a shift, the probability of a shift change during the time window needs to be considered. For a typical HFE time window of 1 hour and a shift length of 12 hours, the probability of no shift change is 1-(1/12) = 0.92, so HFEs by different crew are typically only credited in scenarios in which the HFE time window is longer than the length of a shift.
- **Cognitive.** If the HFEs have a common cognitive element (i.e., performed by the same crew and driven by the same cue or procedural step), the "Yes" branch on the "Cognitive" decision node is selected as a first approximation—because these HFEs would be regarded

as completely dependent. The analyst should determine whether the common cognitive element had been modeled as a separate basic event. If it has, the “No” branch can be selected.

- **Cue Demand.** If the cues for two HFEs occur at the same time, the “Yes” branch on the “Cue Demand” decision node is selected. The required actions for these HFEs are to be performed simultaneously. If the cue for subsequent action occurs before the preceding action can be completed (as shown in Figure 7-2), the “Yes” branch on the “Same Time” decision node is also selected because the required actions would have to be performed simultaneously or the crew may choose to do either one or the other based on some prioritization. These HFEs are termed simultaneous HFEs.

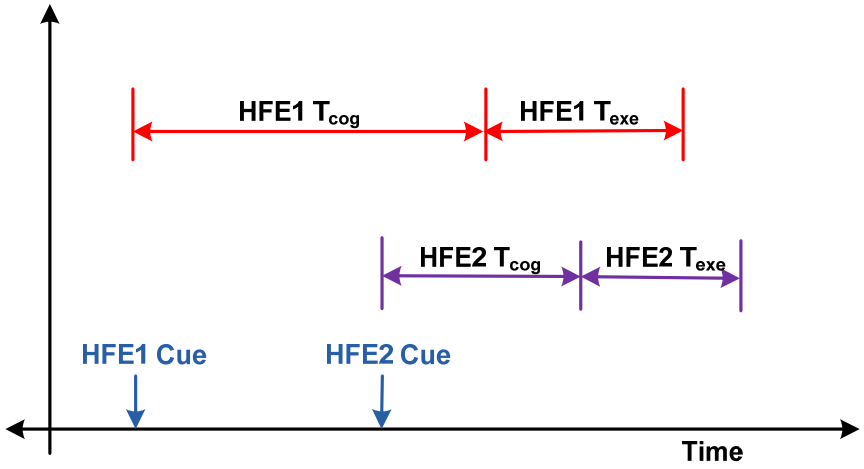


Figure 7-2. Illustration of common cue demands for two HFEs.

- **Manpower.** For simultaneous HFEs, the next consideration is whether there are sufficient resources to support the required actions given the time frame. This determination can be made by comparing the required tasks with the number of crew available. If the resources are inadequate, the “No” branch on the “Manpower” branch is selected, which implies complete dependence. If it can be shown that there are adequate resources to support both HFEs **and** that the scenario is feasible (there is enough time given adequate resources), the “Yes” branch on the “Adequate Resources” branch is selected. Next, location and stress are considered. For the same location, the “Yes” branch on the “Location” decision node is selected. For high or moderate stress scenarios, assign complete dependence; for low stress, assign high dependence. For different locations, the “No” branch on the “Location” decision node is selected. For high or moderate stress scenarios, assign moderate dependence; for low stress, assign low dependence.
- **Location.** Location refers to the room or general area in which the crew members are located. For example, the control room is a location; location is not differentiated down to individual panels in the control room. If the execution of the HFEs occurs in the same location, the dependency level is either high or complete, if the actions are performed in different locations, the dependency level is either moderate or low.
- **Sequential Timing.** This timing decision branch considers the time between the cues. The more time between the cues, the lower the dependency level.
- **Stress.** Stress is a culmination of all other performance shaping factors. These factors may include preceding functional failures and successes, preceding operator errors or successes, potential inappropriate mindsets generated by earlier errors that could still be present, the availability of cues and appropriate procedures, workload, environment (i.e.,

heat, humidity, lighting, atmosphere, and radiation), the requirement and availability of tools or parts, and the accessibility of locations. In general, stress is considered high for loss-of-support-system scenarios or when the operators need to progress to functional restoration or emergency contingency action procedures. The higher the stress level, the higher the dependency level.

With the proper level of dependency identified, the dependent HEPs can be reassessed by applying the appropriate dependency formulas in Table 10-17 in THERP [2], shown here in Table 7-1.

Table 7-1. THERP dependency equations

Dependence Level	***Equation***	***Approximate Value for Small HEP***
Zero (ZD)	*HEP*	*HEP*
Low (LD)	*(1+19 X HEP)/20*	*0.05*
Medium (MD)	*(1+ 6 X HEP)/7*	*0.14*
High (HD)	*(1 + HEP)/2*	*0.5*
Complete (CD)	*1.0*	*1.0*

7.1.3 Additional Dependence Considerations

The IDHEAS general methodology provides a macro-cognition based dependence identification that identify the human failure mechanisms could cause task dependence. The following discussion applies a simplified model that the detecting, understand, deciding, and action macrocognitive functions are performed in sequential order. The discussion of a macrocognitive function is based on the assumptions that its preceding macrocognitive functions are successfully performed. For example, in discussing the understanding macrocognitive function, it is assumed that the detecting macrocognitive function is successfully performed.

Detection macrocognitive function

If HFE1 failed is because failure of detecting a critical piece of information, then the following situations could cause HFE2 dependent failure:

- The critical information in HFE1 is also critical to HFE2, and
- There is no new information shown in HFE2 but not in HFE 1 for the operator to question the correctness of the critical information.

Human heuristics include information convenience heuristic. An individual tends to use whatever information is readily available instead of making efforts to collect the same or similar information.

Example – It take some time to obtain SG chemical sampling results. Once obtained the information the operators may reluctant to request again for the information in the later scenario. Therefore, instead of resampling again for HFE2, the same sampling result obtained in HFE1 is likely to be used for HEF2.

The following are the context factors for assessing the likelihood of dependence:

- □ The information is critical to current HFE and the immediately preceding HFE.

If the above item is checked then check the following that apply:

- □ The procedures or process applied to the event do not request to check the information (e.g., the HFEs could be results of latent failure. The procedures following the initiating event would not request for the information.) The process refers to normal operation requirement such as information gathering in shift turnover.
- □ The information is not readily available but requiring some efforts to obtain.
- □ This is a high pace scenario or a high workload scenario.

Understanding macrocognitive function

If HFE1 failed due to failure in understanding the situation, then the following could cause dependent understanding failure in HFE2:

- The incorrect understanding in HFE1 would cause misunderstanding in HFE2
- No vivid and strong alternative information to alter the course of misunderstanding in HFE2.

Example - In the TMI accident, the operators believed that the RCS was full of water (a misunderstanding based on high PZR water level). The misunderstanding led the operator to systematically defeat the automatic safety functions, e.g., tripping the safety injection and tripping the RCPs.

A note to the readers is that the misunderstanding in this method is under the assumption that no indications were misread; therefore, re-check the same information would not alter the understanding. The following are the context factors for assessing the likelihood of the understanding dependence:

- □ The same misunderstanding that failed HFE1 will fail HFE2.

If the above item is checked then check the following that apply:

- □ New information (e.g., system feedback) is available, which is vivid and strong, to the operators or within the normal process to be obtained by the operators (e.g., in procedure or shift turnover) to question the (mis)understanding.
- □ This is a high pace scenario or a high workload scenario.
- □ No supervisor, overseer or independent checker is available.

Decision-making macrocognitive function

With correct understanding of plant status the operators made conscious wrong decision (e.g., production over safety, incorrectly prioritizing safety concerns, or decision-maker is influenced by the stakeholders who have different considerations from the operators) in HFE1, the same mentality in decision-making could cause dependent decision failure in HFE2. To have the decision dependence the HFE1 and HFE2 have to have the same kinds of decisions such as high economic consequence or priority in protecting RCS or containment. The likelihood of deciding dependence is assessed by the following:

- □ The HFE1 and HFE2 have the same type of decision, e.g.,
  - High economic consequence

- Prioritizing safety concerns between the same barriers (e.g., fuel, RCS/RPV, and containment)
- Influenced by outside stakeholder who have different concerns from the decision makers

If the above item is checked then check the following that apply:

- □ If this decision has high economic consequence: an alternative option that violate the rules of operation but have potential in avoiding or mitigating the economic consequences exist in both preceding HFE and current HFE.
- □ If this decision is about priority between barriers: The two HFEs are prioritizing the same barriers (fuel, RCS/RPV, and containment), and there is no significant differences in treating the integrity of the two barriers between the two HFEs.
- □ The decision is strongly influenced by outside stakeholders who have different considerations from the decision makers.

Action macrocognitive function

The action dependence focuses on the behavior tendency. This type of behavior is considered as individual behavior instead of the team. The rational is that the plant training should prevent this becoming an issue to the overall work force. The likely situation is using a mis-calibrated test equipment to calibrate a group of transmitters. The likelihood of action dependence is assessed by the following questions:

- □ The tasks are performed by the same person or same group of individuals.
- □ The actions are within the same task order or the same procedures.

If both the above items are check then check the flowing that applies:

- □ System, component, or equipment does not provide feedback. Use a mis-calibrated test equipment will result in re-calibrating all equipment. This unusual situation is considered as feedback information.

Cognitive interruption

A cognitive interruption would break the task dependence. In implementation, NUREG-1921 specifies that if two HFEs are separated by an intervening operator successful response, the pair of HFEs are considered independent (or zero dependence). The rationale was that the success HFE represents a cognitive interruption to remove the conditional failure by the same failure mechanism on the sub-sequent HFEs.

In summary, task dependency between HFEs remains as an area for future development. The guidance above provides new insights on dependency factors between tasks based on the underlying cognitive processes. These factors can be used to make a better judgment on the dependency level between two HFEs. IDHEAS-G at present has not developed numeric rules for adjust the HEP values based on the dependency level as those in other HRA methods (e.g., THERP, SPAR-H, and ATHENA).

7.2 Uncertainty Analysis

PRA is a probabilistic model that characterizes the aleatory uncertainty associated with accidents at nuclear power plants (NPPs). This uncertainty is associated with the

incompleteness in the analysts' state of knowledge. NUREG-1855 [5] provides guidance for treatment of three types of uncertainties in PRA: Parameter uncertainty, Model uncertainty, and Completeness uncertainty. The assessment of uncertainty on HEPs is a required part of the PRA.

Parameter Uncertainty: Parameter uncertainty is the uncertainty in the values of the parameters of a model given that the model has been agreed to be appropriate. Current practice as recommended in NUREG-1855 is to characterize parameter uncertainty using probability distribution of the parameters in the model. Regarding multiple parameters involved in a model, NUREG-1855 states “When the parameters are combined algebraically to evaluate the PRA numerical results or some intermediate result such as a basic event probability, these uncertainty distributions can be mathematically combined in a simple way to estimate the uncertainty of those numerical results.” IDHEAS-G adopt NUREG-1855 recommendation on three ways to estimate the probability distribution of model parameters.

Model Uncertainty: NUREG 1855 describes that “Model uncertainty is related to an issue for which no consensus approach or model exists and where the choice of approach or model is known to have an effect on the PRA model (e.g., introduction of a new basic event, changes to basic event probabilities, change in success criterion, and introduction of a new initiating event). A model uncertainty results from a lack of knowledge of how SSCs behave under the conditions arising during the development of an accident.” Therefore, “It is necessary to demonstrate that the key uncertainties, reasonable alternative hypotheses, or modeling methods would not significantly change the assessment.” NUREG-1855 recommends that treatment of model uncertainty should be performed by identifying key sources of model uncertainties and related key assumptions relevant to the base PRA and the risk-informed decision under consideration, then performing sensitivity analysis to understand the impact of the key sources.

IDHEAS-G provides guidance on developing application specific HEP quantification models from its Basic Quantification Structure. In the development of a quantification model, many assumptions are made about the application. . For example, one assumption for the quantification model of IDHEAS internal at-power application is that that the set of CFMs and PIFs is adequate to represent the potential crew failure modes and PIFs in internal at-power events. Yet, there could be other CFMs and PIFs that are significant in an unusual event within the scope. Guidance on dealing with this type of uncertainty in risk-informed applications essentially focuses on changing the HEP values en masse to determine whether the assumed HEP values mask other risk insights (which would occur if they were considered to be conservative) or underplay the role of the operators (if the HEP values were considered to be too low). However, what can be examined more straightforwardly is the effect of the assumptions that are made in applying the method, e.g., deciding whether a PIF is nominal or poor Similarly, there may be uncertainties associated with the assessment of the time factors that are used to assess feasibility and particularly with respect to whether recovery is feasible. These types of uncertainties can be explored within IDHEAS by the performance of sensitivity studies that explore the effect on the HEPs of taking alternate paths through the decision trees. Such studies can provide useful input to identify those PIFs that are most critical to the determination of the significance of an HFE, and are candidates for improvement of plant practices or procedures.

The sensitivity analysis determines whether the acceptance guidelines (used in the decision-making) are challenged. NUREG-1855 recommended an acceptable approach to treat model

uncertainty in HRA is “to perform a sensitivity study varying all the HEPs by the same factor. The magnitude of the factor should be chosen taking into account a number of issues, including the uncertainty range dictated by the HRA method, but also a comparison of the HEPs derived for similar HFEs in different PRAs using different HRA methods. This should be done both. For an increase in the HEPs and by a decrease for the following reasons. An optimistic evaluation of the HEPs can lead to the lessening of the importance of the SSCs that appear in the same cut sets or accident sequences as the corresponding HFEs. On the other hand, a conservative evaluation can lead to masking the importance of other contributors, particularly those in cut sets and sequences not involving the HFEs.”

Completeness Uncertainty: Completeness uncertainty arises from those contributors that have not been included in the scope of the PRA. NUREG-1855 states “Lack of completeness is not in itself an uncertainty, but recognition of the limitations in the scope of the model. However, the result is an uncertainty about where the true risk lies. It represents a type of uncertainty that cannot be quantified and because it represents those aspects of the system that are, either knowingly or unknowingly, not addressed in the model. The true unknowns (i.e., those related to issues whose existence is not recognized) cannot be addressed analytically. However, in the interests of making defendable decisions, these unknowns are addressed during the decision-making. The principles of safety margins and defense in depth play a critical role in addressing this source of uncertainty.” The guidance recommends to use screening and conservative analyses to address the significance of the contributors and screen out the non-significant contributors.
Addresses completeness uncertainty during the decision-making is beyond the scope of this report. Yet, the IDHEAS General Methodology gives it considerations in the preparation step and the beginning step of scenario analysis for known contributors. In these steps, the HRA analysts work with the PRA team to determine the analysis scope, the event boundary conditions and termination criteria, and the systems or components that should be included in the analysis. In these steps, the HRA and PRA team explicitly or implicitly perform some kinds of screening analysis to demonstrate that a particular item (e.g., a hazard group, an initiating event, a component failure mode, etc.) can be eliminated from further consideration in a PRA being used to support a risk-informed application. This screening can be accomplished by showing that either the item has no bearing on the application (qualitative screening) or that the contribution of the item to the change in risk associated with the application is negligible (quantitative screening). Furthermore, the process of identifying HFEs is a qualitative screening process by identifying only those HFEs that have impacts on plant safety. This is further manifested by the HFE feasibility analysis. In addition, the General Methodology also provides guidance for conducting a quantitative screening analysis for HFEs.

Active research is ongoing in the area of uncertainty analysis for HRA; the following additional references should also be considered:

- EPRI 1009652 [6]
- NUREG-1792 [3]
- NUREG/CR-1278 [2]

8 References

1. ASME/ANS RA-Sa-2009, Addenda to ASM/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 2009.
2. Swain, A. D. & Guttman, H. E. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. (NUREG/CR-1278, SAND80-0200). Washington, DC: U.S. Nuclear Regulatory Commission.
3. Kolaczkowski, A., Forester, J., Lois, E., & Cooper, S. (2005). Good Practices for Implementing Human Reliability Analysis (HRA). (NUREG-1792). Washington, DC: U.S. Nuclear Regulatory Commission.
4. EPRI/NRC-RES Fire Human Reliability Analysis Guidelines (2012). (EPRI-1023001/NUREG-1921). EPRI, Palo Alto, CA, and U.S. Nuclear Regulatory Commission, Washington, DC.
5. Drouin, M., Parry, G., Lehner, J., Martinez-Guridi, G., LaChance, J., & Wheeler, T. (2014). Guidance on the Treatment of Uncertainties Associated with PRAs in Risk-Informed Decision Making. (NUREG-1855). Washington, DC: U.S. Nuclear Regulatory Commission.
6. Guideline for the Treatment of Uncertainty in Risk-Informed Applications: Technical Basis Document (2004). (EPRI 1009652). Palo Alto, CA: Electric Power Research Institute.

Appendix A: Cognitive processes, CFMs, and associated cognitive mechanisms

Appendix A contains the cognitive process, CFMs, and associated cognitive mechanisms for every macrocognittive function. All the cognitive mechanisms are listed at the bottom section for each macrocognitive function and are labeled in capital letters; the mechanisms associated with a step of the cognitive process are referenced with the letters in the last column of the table.

DETECTION			
Cognitive process	**Proximate cause**	**Cognitive failure mode (CFM)**	**Cognitive mechanism**
D1- Initiate detection - Establish mental model and criteria for information to be acquired	Fail to Initiate detection	D1-1 *Detection not initiated (e.g., Skip steps of procedures for detection, forgot to check information, no instruction for detection)* D1-2 *Wrong detection criteria used* *D1-3 Fail to prioritize information to be detected*	AB
D2 - Identify and assess equipment needed	Fail to identify and assess equipment needed	D2-1 *Fail to prepare the right measurement equipment / detection tools, or inspection systems (equipment incorrectly identified; unable to operate equipment,; incorrect calibration of the equipment)*	C
D3 – Identify and attended to sources of information	Fail to identify and attended to sources of information	D3-1 *Fail to access the source of information (fail to access, view, or measure partial or all sources, motor failure in probe movement to sub-areas for detection)* D3-2 *Wrong source attended*	ABDEF
D4- Perceive information	Incorrectly perceive information	D4-1 *Key alarm not attended to* D4-2 *Fail to recognize that primary cue is not available or misleading* D4-3 *Cues (abnormals) not perceived* D4-4 *Cues misperceived (information Incorrectly perceived, fail to perceive weak signals, reading errors)* D4-5 *Fail to monitor status (e.g., Information or parameters not monitored at proper frequency or for an adequate period of time, fail to monitor all the key parameters, incorrectly perceiving the trend of a parameter))*	DEFG

D5- Recognize, verify, and confirm information acquired	Incorrectly recognize information	D5-1 *Incorrectly interpret, organize, or classify information*	GHIJ
D6- Communicate the acquired information	Fail to communicat e the acquired information	D6-1 *Detected cues not retained or incorrectly retained (mark wrong items, wrong recording, wrong data entry)* D6-2 *Cues not communicated or* miscommunicated	JK

Cognitive mechanisms for Detection:

A. Mental model about the cures - No mental model about the cues; Expectation is wrong or biased

B. Detection criteria – Ambiguous criteria; unable to match information to criteria

C. Sensory process – human sensory (visual, aural, olfactory, somatosensory, etc) system not fitting for the detection, sensory system aids (tool or equipment to detect information) not working properly;

D. Information foliage (filtering) - low signal-noise ratio of information content

E. Vigilance - Loss of vigilance, attenuation

F. Attention - Attention is not focused on cues; attention is not shifted properly; Unable to maintain attention for a long duration

G. Working memory – Memory overflow; Memory degraded with time; Memory not consolidated; Memorizing wrong information

H. Teamwork - Inadequate supervision

I. Teamwork - Inadequate work process for peer-checking and confirmation

J. Information retaining - Perceived information not retained in working memory or recorded

K. Lack of communication

UNDERSTANDING

Cognitive process	Proximate cause	Cognitive Failure Mode	Cognitive mechanism
U1 - Assess/select data	Fail to Assess or select data	U1-1 *Incomplete data selected (e.g., critical data dismissed, critical data omitted)* U1-2 *Incorrect or inappropriate data selected (e.g., fail to recognize the boundary conditions of data, not recognize information age)*	A-E

U-2 Select / adapt / develop the mental model	Incorrect mental model	U2-1 *Incorrect mental model selected* *U2-2 Fail to recognize mismatched procedures (e.g., fail to adapt procedures)*	F-J
U-3 Integrate data with mental model to generate understanding (situation awareness, diagnosis, resolving conflicts))	incorrect integration of data and mental model	U3-1 *Incorrectly assess situation (e.g., Situational awareness not maintained, Incorrectly predict system evolution or upcoming events)* U3-2 *Fail to or Incorrectly diagnose problems (e.g, Conflicts in data not resolved)* U3- 3 *Fail to use guidance outside main procedure steps (e.g., fold-out pages) in diagnosing*	K-R
U-4 Iterate the understanding - Verify and revise the understanding	Fail to iterate the understan ding	U4-1 *Premature termination of data collection (e.g.,* Not seek additional data to reconcile gaps, discrepancies, or conflicts, Not revise the outcomes based on new data, mental models, or view points) U4-2 *Individual's biased or incomplete understanding accepted by the team (e.g.,* assessment or diagnosis not verified or confirmed by the team, lack of confirmation and verification of the results in the work process*)* *U4-3 Fail to generate coherent team understanding*	STU
U-5 Communicate the outcome with other parties	Fail to communica te the outcome	U5-1 *Outcomes of Understanding miscommunicated or inadequately communication*	VW

Cognitive mechanisms for Understanding:

A. Information available in the environment (including procedures) is not complete, correct, or otherwise sufficient to create understanding of the situation

B. Attention to wrong or inappropriate information

C. Improper data or aspects of the data selected for comparison with or identification of a frame

D. Incorrect or inappropriate or inadequate frame used to search for, identify, or attend to information

E. Data not properly recognized, classified, or distinguished.

F. Incorrect or inadequate frame or mental model used to interpret or integrate information

G. Frame or mental model inappropriately preserved or confirmed when it should be rejected or reframed

H. Frame or mental model inappropriately rejected or reframed when it should be preserved or confirmed

I. Incorrect or inappropriate frame used to search for, identify, or attend to information

J. No frame or mental model exists to interpret the information or situation.

K. Data not properly recognized, classified, or distinguished

L. Improper integration of information

M. Improper aspects of the frame selected for comparison with the data

N. Improper data or aspects of the data selected for comparison with or identification of a frame

O. Incorrect or failure to match data or information to a frame or mental model

P. Mental manipulation of the information (including projection of future status) is inadequate, inaccurate, or otherwise inappropriate

Q. Working memory limitations impair processing of information

R. Improper control of attention.

S. Failure of team communication in the process of Understanding

T. Inadequate leadership/supervision

DECISION-MAKING

Cognitive process	**Proximate cause**	**Cognitive Failure Mode**	**Cognitive mechanism**
DM1 – Manage the goal	- *Incorrect Goals or Priorities Set*.	DM1 – 1 *Incorrect goal selected* DM1 – 2 *Incorrect prioritization of goals*	ABC
DM2 – Select or develop a decision model to meet the decision goals and criteria	Inappropriate decision model	DM2 – 1 *Incorrect decision model* (e.g, heuristic is used, no decision-model meets the goals) DM2 – 2 *Incorrect decision criteria*	DE
DM3 – Acquire / select information to be used for DM	Information is under-represented	DM3 – 1 *Critical information not selected or only partially selected (e.g., under-sampling information)* DM3 – 2 *Selected information is not appropriate (e.g., out dated, not applicable for the situation)*	FG

		DM-3 Misinterpret or misuse selected information	
DM4 - Make decision (judgment, strategies, plans)	*- Incorrect Internal Pattern Matching*.	DM4 – 1 *Misinterpret procedure* DM4 – 2 *Choose inappropriate strategy* DM4 – 3 *Incorrect judgment* DM4 – 4 *Incorrect or inadequate planning or developing solutions (Plan wrong or infeasible responses, Plan the right response actions at wrong times, Not plan configuration changes when needed, Plan wrong or infeasible configuration changes)* DM4 – 5 *Decide to interfere or override automatic or passive safety-critical systems*	HIJKLM
DM5 - Simulate / evaluate the decision / plan	Fail to simulate / evaluate the decision / plan	DM5 – 1 *Not or unable to simulate or evaluate the decision (not assess negative impacts, unable to evaluate the pros and cons)* DM5 – 2 *Incorrectly simulate or evaluate the decision (e.g., not evaluate the impact on other related system or components, not consider all the key factors)*	NOPQR
DM6 - Communicate and authorize the decision	Fail to communicat e or authorize the decision	DM6 – 1 *Decision not properly communicated* DM6 – 2 *Decision not authorized or delayed authorized (e.g.,* unable to authorize the decision due to ambiguity or problems in authority)	STU

Cognitive mechanisms for Decision-making:

A. lack of goal prioritization. Goals may be ordered incorrectly in the operators' mind or given the wrong priority, such that less important goals are addressed first.

B. Incorrect judgment of goal success. The threshold used by the operator to judge goal success may be incorrectly set too low, or be incorrectly determined as met when it was not.

C. Not updating the mental model to reflect the changing state of the system.

D. Fail to retrieve previous experiences.

E. Incorrect recall of previous experiences.

F. Incorrectly comparing the mental model to previously encountered situations.

G. Cognitive biases. Confirmation bias and availability bias may be particularly pertinent to causing errors in this phase of decision making

H. Inaccurate portrayal of action. Incorrect inclusion of alternatives. The operator may forget to include some alternatives that should be considered.

I. Inaccurate portrayal of the system response to the proposed action.

J. Overconfidence and anchoring. Overconfidence affects the operator's confidence in the ability of an action to work. Especially if the operator has had previous success with an action, he or she may be overconfident in its ability to work in the present case. The anchoring effect states that people are biased toward the first option they see or the first judgment they make. Therefore, an operator may be biased toward choosing the first action that occurs to him or her, and apply an unsuitable action.

ACTION EXECUTION

Cognitive process	**Proximate cause**	**Cognitive Failure Modes**	**Cognitive mechanism**
E1–Assess action plan	Fail to assess action plan	E1-1 *Incorrectly assess or interpret the action plan (e.g., errors in personnel allocation, equipment / tool preparation, or coordination)* E1-2 *Wrong action criteria developed*	A B C D X
E2 - Develop / modify action scripts	Fail to develop / modify action scripts	E2-1 *Incorrectly modified or developed action scripts for the action plan* E1-2 *Incorrectly add action steps to manipulate safety systems outside action plans (e.g., error of commission)*	A B C D E X
E3–Synchronize, supervise, and coordinate action implementation	Failed to coordinate action implementation	E3-1 *Delayed implementation* E3-2 *Action not initiated (e.g., Fail to coordinate actions, Not perform the plant status checking required for initiating actions, Failed command & control)*	D E U V W X
E4 - Implement action scripts	*Failed to take planned action*	E4-1 Fail to follow procedures (e.g., *Skip steps in procedures*) E4-2 *Fail to execute skill-of-craft actions* *E-3 Fail to execute simple action* E4-4 *Fail to execute complex action (Execute all the steps of a complex action in wrong timing or sequence, Execute actions that do not meet the entry conditions, Not or mis-coordinate execution of complex actions among team members)*	B through U

		E4-5 *Fail to execute long-lasting actions* *E4-6 Fail to execute fine-motor actions*	
E5 - Verify and adjust actions	Fail to verify or adjust action	E5-1 *Fail to adjust action by monitoring, measuring, and assessing outcomes* *E5-2 Fail to complete the entire action plan (e.g., omit steps after the action criteria are met)* E5-3 *Fail to record, report or communicate action status or outcomes*	E J K L S T U V

Cognitive mechanisms for Action:

A. Action criteria - Population stereotypes
B. Action criteria – Mismatch between criteria and actions
C. Physical fitness
D. External tools to aid physical fitness
E. Automaticity control – Automaticity stereotype
F. Motor learning - Learning un-stabilized
G. Negative transfer/habit intrusion
H. Central executive control – Dual-task or multitasking interference
I. Attention – Loss of attention (Attention not maintained or not focused on task; Lack of attention control or attention shit
J. Lack of Vigilance
K. Working memory – Working memory overflow, not consolidated, decay over time, interfered with similar information or past experience
L. HSI - Indicator mode confusion
M. HSI - Recognition errors
N. Manual control
O. Continuous control deficiencies
P. Motor speed-accuracy trade-off
Q. Fitt's Law of motor movement - the time required to rapidly move to a target area is a function of the ratio between the distance to the target and the width of the target.
R. Error monitoring and correction
S. Stimulus response compatibility
T. Failure of communication during action execution
U. Inadequate supervision and peer-checking
V. Inadequate coordination

Appendix B: A Comprehensive list of PIFs

Appendix B contains a comprehensive list of PIFs for every macrocognitive function. The fist column of the table indicates the steps of the cognitive process, using the same labels as those in Appendix A. The cognitive mechanisms that link the PIF to the step of the cognitive process are also indicated in the first column using the same labels as those in Appendix A. The second column of the table are the PIFs. For every macrocognitive function, the PIFs are presented in three sections: The first section are the error contributing factors that directly contribute to the HEP; the second section are the modification factors that affect all the steps of the cognitive process; the third section are the modification factors that are specific for the CFMs under a step of the cognitive process.

Cognitive process / Mechanisms	**PIF for Detection**
All steps D1-D6	**Error contributing factors** • Information reliability - Sensors or indicators may be unreliable (e.g., damaged, degradation, false alarms in design, out-of-range, inherently unreliable sources, problems in communication, or flaw in system state indication) • Information signal is weak or masked (visually or aurally) • Primary sources of information are not available while secondary sources of information are not reliable, perceivable, or understandable • Detection criteria are complex (e.g., multiple criteria to be met or in complex logic) • Criteria are not applicable to the information • Criteria are ambiguous
	Modification factors
	Unfamiliar scenario
	Intermingled multitasking
	Frequent or persistent interruption/distraction
	Unpredictable system dynamics
	Cognitive complexity in detection – Information demands may exceed the individual's working memory capacity: o Concurrently monitor 3 or more than 3 non-related developing situations. o Concurrently monitor 7 or more parameters o Mentally retain multiple pieces (> 7) of information
	Time pressure and other stresses

	Mental fatigue o Long working hours under stress or in harsh environment o Sustained high-demanding cognitive activities (e.g., information changes over time and requires sustained attention to monitor or check at a certain frequency for a long period of time.
D1 –A	Procedure, guidance, or instruction for detection is inaccurate or inadequate - o Multiple guidance documents must be referenced or open at the same time o No place-holders to maintain one's place in the document o Document nomenclature does not agree with equipment labels
D1 –AE	Expectation on information detection is biased
D2 – A	Unfamiliar with the equipment or tools needed for detection
D2 - A	Lack of training on failure modes of the equipment or tools
D3 - BCDEF	The information source is similar to other sources nearby
D3 –B	Information source is obscured due to environment factors o Labels on the source are difficult to read
D3 –BE	Inexperienced with sources of information
D4 –B	CLARITY: Confusion of indications or un-intuitive indications. The indication or label can be interpreted differently for reasons such as imprecise in axis labeling in an X-Y plot
D4 –BF	The process needed to obtain the information, e.g., the information of interest has to be determined based on the status of other pieces of information. o The number of information needs to be checked to determine the information of interest: o Involve 2 or more than 2 types of logic operators (e.g., AND, OR, NOT, and NOR.)
D4 –BCD	SALIENCE: The information has similar appearance with surrounding information o The information to be detected is buried in a large amount of potentially relevant information. o The information cannot be easily identified because the environment causing visual or auditory camouflage. o The information has human factors issues (e.g., font is too small and located too far and poor lighting, misuse of colors, etc.) o Visibility of information is low due to environmental factors

D4 –CD	PROLONGED ATTENTION: Information changes over time and requires sustained attention (> 10 minutes). o Determining a parameter trend during unstable system status that required continuous attention for more than 10 minutes. For example, determining the RPV temperature trend in the situations of water just injected into the RPV. It would take some time to see the stable temperature trend. o Monitoring a slow-response-system's behavior without clear time window to conclude the system response/behavior.
D4 –BD	Training: Inadequate training on urgency / criticality of key information such as key alarms
D5	
D5 -GH	No peer-checking or cross-checking
D5 -GH	The related information to verify the information of interest is not available, not immediately available, or not salient.
D5 -GH	The same information cannot be detected by individual(s) at a different location (e.g., the information appears in the main control room and on site during refueling outage).
D5 -GH	Inadequate supervision - An overseer or independent reviewer is not available.
D5 -GH	Unfamiliar with the failure modes of the information sources
D5 -GH	Lack of safety / risk-prevention attitude at work
D6	
D6 -IJK	Communication equipment and protocol: o Communication requires operating unfamiliar, special equipment o Involve Multi-modalities (audio from pilot, audio from supervisor, visual information from various information sources) o Different communication protocols between the communication parties (e.g., three-way communication requirement is a protocol.) o Routine communication means could be partially or fully disabled o Communication equipment degradation (e.g. due to environmental factors) o Reduced effectiveness of information transmission (e.g., due to noise, storm)
D6 -JK	Communication complexity: o Involve three or more than three sites, parties o Unfamiliarity of communication parties (e.g., required to communicate with offsite support party that has less than once per year joint drill.)

	○ Content complexity
Cognitive process	**PIFs for Understanding**
All process steps U1-U5	**Error contributing factors** • Incomplete information from system to understand the situation (I&C failure, malfunction, loss of some sources of information due to environmental factors, Transition in system control state is not acknowledged) • Inadequate updates of plant information due to infrastructure (could be the information perceived by a party (e.g., MCR) but failed to inform another party (e.g., TSC)) • Pieces of Information change over time at different paces thus they become uncertain by the time they are used together for Understanding. • No existing mental model for the situation • Procedures or guidance is inadequate to develop a mental model of the situation; Crew has to rely on knowledge to develop a mental model • Information /Cues and do not match procedures / guidance (No obvious answer – can have multiple explanations) - There are multiple, alternative, explanations for the pattern of symptoms observed.
	Modification factors
	Unfamiliar scenario
	Intermingled multitasking
	Frequent or persistent Interruption/distraction
	Unpredictable system dynamics - System behavior may be unexpected and unexplained.
	Cognitive complexity in Understanding ○ Multiple explanations - There are multiple independent 'influences' that are simultaneously present and in combination explain the observed data ○ The information is distributed spatially or over the time thus it demands working memory and attention to retain and combine the information. ○ Information of varying levels of importance is mixed and the relationship of the pieces of information is unclear ○ Key information is logically masked - (hidden coupling, cascading effects, cognitive masking, complex logic) - A source of a problem is difficult to detect because of cascading secondary effects that makes it difficult to connect the observed symptoms to the originating source.
	Time pressure and other stresses

	Mental fatigue - Long hours at work or long period of sustained cognitive activities
U1 – Assess data	
U1-ABCDE	Sources and meanings of data are unfamiliar - thus data may not be selected.
U1-AD	Inadequate experience on collecting all the relevant information for understanding
U1-ABD	Guidance is not specific in searching for additional / redundant information when the primary cues are not available or not reliable.
U2 - Select /mental model	
U2 - FGHIJ	Anchoring bias - The mental model is correct for most situations but is not correct for the specific situations (Stereotype violations (Not the usual suspect – In most situations, there is a stereotypical explanation for a set of data. In this scenario, the 'usual suspect" explanation is not the best explanation.)
U2 – FGHIJ	Not familiar with detail system design and how the system works in the specific
U2 – FGHIJ	System/HSI failure modes or negative impacts may not be anticipated by operators (and designers).
U2 –FGH	
U2 –FGH	Information requires specialized expertise in order to appreciate the significance
U2 -J	No or inadequate guidance, tools, or procedures for diagnosing the problems
U2 -J	Understanding the scenarios requires integration of diverse knowledge/ expertise beyond individual crew members' scope
U3 – Integrate	
U3 –LNO	Available information conflicts or does not converge to reaching to a coherent understanding of the situation.
U3 –PQR	Complex calculations or logic reasoning involved (e.g., procedure is not specific for the situation the operator had to fill in the details to make the procedure works for the situation)
U3 –LMN	Work process is poor in reconciling different viewpoints

U3 –PQR	Complex logic to follow in guidance - Sequential presentation of guidelines requires the crew to go through several loops before finding the correct indications to diagnose the plant status
U3 –PQR	Multiple guidance documents are needed simultaneously
U4 –TU	Inadequate leadership in facilitating discussion and avoiding tunnel vision (e.g., the team is newly formed)
U4- S	Lack of questioning attitude through training and experience
U4-T	Gaps in team knowledge and expertise needed for understanding the scenario
U4-STU	Under-experience in diagnosis (not being aware of and coping with biases, not seeking additional information, not avoiding tunnel-vision, etc)
U4-STU	No supervision / leadership to initiate and supervise verification / questioning
U4-STU	No independent checking or critique (such as the STA roles)
U5 -VW	Lack of or ambiguous requirements for communicating assessment within team and with other parties
Cognitive process	**PIFs for Decision-making**
All steps DM1 – DM6	**Error contributing factors for decision-making** • Inadequate or partially wrong information for decision-making • Uncertainties in the information - Sources and reliability of information are uncertain to decision-makers • Decision Criteria are not available • Decision Criteria are not applicable to the decision goals • Decision Criteria are ambiguous and subjective to different interpretation
	Modification factors
	Unfamiliar scenario
	Intermingled multitasking
	Frequent or persistent Interruption/distraction
	Unpredictable system dynamics
	Cognitive complexity for Decision-making o Multiple, intermingled goals or criteria to be met o Decision-making requires integration of a variety types of information with complex logic. o Dynamic-decision-making - Complex system dynamics that require constantly collecting information and adjusting the decision.

	o Organizational complexity in decision-making (too many levels of authorities, inter-locked authority entities, verity of entities involving in decision-making)
	Timing pressure and other stresses
	Mental fatigue (Long working hours or sustained cognitive activities)
DM1 – manage goals	
DM1 -AB	Conflict goals: choose one goal will block achieving another goal; Multiple competing goals cannot be prioritized
DM1-ABC	Competing strategies: Multiple strategies can achieve the same goal but with different benefits and drawbacks. These strategies affect each other (e.g., competing resources or delaying critical actions that affect success likelihood).
DM1- BC	No procedure/guidance available for making the decision; (e.g., procedures or guidance does not applicable to the situation)..
DM2 –DE	Inadequate procedure/guidance: o Procedure/guidance does not provide sufficient details for smooth decision making. Judgments are needed to supplement the lack of procedure details. o Conflicting guidance in procedures, policies, or practice on making the decision. o Does not provide warnings about the pitfalls related to the decision.
DM2 –DE	Distributed decision-making: Decision model needs to be developed by groups with different situational awareness, expertise, and at different locations
DM3-FG	
DM3 –FG	Unfamiliar with sources of information (e.g. scope and limitation of data, information age)
DM3 –FG	Unable to conduct a walk-through of the work site
DM3 –FG	Inadequate training on avoiding heuristics
DM3 -FG	Information is not well organized and overwhelming for decision-makers to select
DM4 – KLN	Bias or preference for wrong strategies exists
DM4 – KLN	The situation mismatched with prior training/experience.
DM4 -HIJ	Not familiar with the available resources (equipment and manpower).

DM4 – IJKMN	Making the decision requires multiple expertise distributed among multiple individuals/parties who may not share the same information and understanding of the situations\
DM4 -HM	Key decision-maker's inadequate qualifications or experience
DM4	Inadequate team cohesion (lack of understanding each other, lack of required knowledge or experience in the team, Not having a clear designated decision maker on the scene not well-defined roles and responsibilities of team members)
DM5 – NOPQ	Unable to evaluate strategy effectiveness (e.g., pros vs cons)
DM5 – NOPQ	The decision has unintended side effects which are hard to predict in advance.
DM5 – NOPQ	Feedback Information is not available in time for correcting a wrong decision or adjusting criteria / strategies.
DM5 - NOPQ	Shifting objectives - The tasks originally given to operators change over time, due to shifts in objectives, detection by others of violated assumptions, or the need to synchronize with other personnel who did not accomplish everything according to the original plan. This requires a revision in plan to meet original goals/intent.
DM6-R	No clear guidance for the content of communication for different purposes (e.g., communication to upper or lower levels, with other parties).
DM6 -R	No guidance or protocol on communicating the decisions
DM6 - ST	Authorization complexity – levels and roles of authorization entities
DM6 -ST	The involved parties has not been trained or drilled together.
DM6 -ST	Crew coordination difficulty: o Does not state what to do if equipment is initially operating outside of the range specified in the procedure o Does not warn of all conditions that should be avoided during procedure performance o Insufficient provision of contingency steps o Unclear logic such that the operators are likely to have trouble identifying a way to proceed forward through the procedure
Cognitive process	**PIFs for Action execution**
All steps	**Error contributing factors** • Location accessibility (travel paths, security barriers, and sustained habituation of worksite) • Visibility of worksite

E1– Verify action plan E2 - Develop action scripts E3 - coordinate action E4 - Implement action scripts E5 – Adjust action	• HSI / Tools / Equipment operability (degradation, reliability, calibration, compatibility) • Resistance to motor movement (wearing heavy cloths, lifting heavy materials, opening/closing o rusted or stuck valves, executing actions in water / high wind / extreme coldness or hotness or on unstable ground) • Requirements for high accuracy fine motor skills or fine motor coordination • Criteria for actions are not available • Criteria for actions are infrequently trained or Operators rarely perform the actions • Action criteria are difficult to use (e.g., no indication that the criteria are met, criteria not explicit or concrete, or too complicated to follow)
	Modification factors
	Unfamiliar scenario
	Intermingled multitasking
	Frequent or persistent interruption/distraction
	Unpredictable system dynamics
	Action complexity o # of action sequences o Size of action sequences (# of non-automatic action steps) o # of simultaneous and intermingled action sequences o # of continuous actions (relying on system feedback) o # of exceptions
	Time pressure and other stresses
	Fatigue (Long-time in work, time of the day, and persistent high-level cognitive activities)
E1– C	Reluctance to execute the action plan due to potential negative impacts (e.g., personnel injury)
E1– X	Inadequate leadership to initiate assessment of action scripts
E1–U	Unable to verify the plan because of inadequate communication (of the goals, negative impacts, deviations) with decision-makers
E1–ABE	Training focuses on procedure-following without encouraging operators/leaders to interpret / confirm action plans
E1–ABEWX	Inappropriate crew assignment – under-staffing, lack of skills, limited access to the action sites
E2 - E	Unfamiliar with system failure modes

E2 - ABCDE	Procedures do not completely match the situation (e.g., damaged or degraded HSI due to environmental factors)
E2 - M	Inadequate organizational culture to take responsibilities that current scripts / rules do not fit
E2 - W	Inadequate coordination between site personnel and decision-makers to adapt or modify action scripts based on site situation
E3– W	Unclear staff role definitions
E3–W	Unfamiliar, distributed, or unstable operational teams
E3–CD	Unfamiliar with work sites
E3 - UWX	Action needs coordination between multiple parties at different locations
E3 - U	Communication difficulty (protocol, equipment, complexity) for coordinating actions
E3 - JKLP	Initiation of the action requires to monitor certain parameters over a period of time or wait for a period of time (until the parameters reach the given status)
E4 - JKLP	Actions demand on prospective memory (Delayed follow-up activity) – action scripts include disconnected activity in the future for which there is no strong memory cue, action scripts requires to memorize past status over a long period of time (> several hours)
E4 - JKLQR	Timing issues in following the scripts (Out of sequence steps)
E4 - M	Mode confusion – An intended response to a stimulus probe requires an unnecessary translation to a different side, modality, or navigation to a different physical or conceptual space.
E4 - H	Negative Transfer between tasks (Not used to doing it this way) – Identical or similar tasks done in different settings, modes, or procedural sequences require different approaches.
E4 - EFGH	Staff are under-training for the types of actions
E4 - GAKL	The action requires skill-of-craft
E4 - F	Unlearn or break away from automaticity of trained action scripts
E4 -	No existing procedures / guidance / instruction for action scripts
E4 -	No experience or adequate learning for action scripts
E4 - QOPT	Controlled actions that require monitor action outcomes and adjust action accordingly
E4 - E	Procedure logic or layout makes it difficult to follow the procedure step-by-step

E4 - IJOPQR	Environmental factors (e.g., wind, storm, ambient temperature) make fine motor actions difficult
E5 - V	Inadequate supervision in monitoring actions and questioning current mission
E5 - W	Unable to keep global overview because of team distribution
E5 - STU	Inadequate HSI o Lack of feedback from system to crew o Lack of adequate confirmation of actions o Confusion in action maneuver indications

Appendix C: Demonstration of IDHEAS-G

This appendix documents the analysis results of the FLEX Mitigation Strategies for an Extended Loss of ac Power (ELAP) and the Loss of Ultimate Heatsink (LUHS) Event

Document the outcomes of Step 1 "Scenario analysis and operational narrative"

Initial condition: A Boiling Water Reactor (BWR) at 100% power operation
Initiating event: ELAP and LUHS induced by a Beyond Design Basis earthquake
Boundary condition: Large scale site damage as specified in NEI 12-06. Some highlights are:

- The event occurred when the staffing is at the minimum emergency plant staffing level.
- No site accessibility within the first six hours after the initiating event.
- No other major concurrent events (e.g., Spent Fuel Pool damage, external flood, large fire or security events)

Consequences of interest: radioactivity release to outside of containment

Description of scenario: *Event progression described in timeline and narrative stories*

The beyond design basis earthquake caused a two BWR reactors site to experience a combination of an extended loss of ac power (ELAP) event and a loss of ultimate heat sink (LUHS) event The earthquake caused site wide damage and limited site access for a period of time. The High Pressure Coolant Injection (HPCI) and Reactor Core Isolation Cooling (RCIC) systems functioned as expected following the earthquake. Immediately after the event, the operators are expected to know that this is a Station Blackout (SBO) event. The immediately required tasks are to ensure that the Reactor Pressure Vessel (RPV) has sufficient cooling (in this case, the RPV is cooled by RCIC), restore the ac power, and shed the dc load. After unsuccessfully restarting the Emergency Diesel Generators (EDGs) and not expecting the offsite power to be restored within an hour, an ELAP event is declared. This declaration led to the performance of the deep dc load shed procedure, and mobilization of the FLEX equipment (portable generators, portable pumps, and portable fans, etc.) to prolong RCIC operation and to have a redundant means to cool the core if case the RCIC and HPCI failed. The operators are expected to request additional equipment, if necessary, from the national resource center. The earliest shipment of the equipment and personnel to supervise the assembly, setup, and operate the equipment from the regional resource center is expected to be 24 hours after the event.

See Table X below for the timeline and operating experience.

Scenario context

Before the earthquake, the two units are at full power operation. The earthquake caused site wide damage that damaged most of the structures that are not seismically robust. The following highlights the significant effects. The detailed effects can be found in NEI 12-06:

- ELAP and LUHS

- No site accessibility within the first 6 hours of the event; limited site access within the first 24 hours; and having full site accessibility after 24 hours.
- The steam driven HPCI and RCIC function as expected. The default water source, condensate water storage tank whose piping is not seismically robust, is damaged by the earthquake but the alignment successfully automatically transfers the suction water to the torus because of the low suction pressure signal.
- Without shedding the dc load, the essential batteries are expected to exhaust within two hours. With the initial dc load shed, the batteries are available for 5 hours. A deep dc load shed will increase the battery availability to 7 hours.
- When the RPV water level reaches the low level set point, the RCIC will automatically inject water into the RPV. When the RPV water level reaches the high level set point, the RCIC flow will be automatically shutoff. Therefore, when the RCIC function normally, the RPV water level is between the low level set point and the high level set point.
- The 2 psig of containment pressure entry point into the Containment Control Process is reached within 30 minutes after the initiating event.
- Because of the loss of torus cooling, the torus will gradually heat up. When the torus water temperature reaches 230°F, the RCIC is assume failed. Without early venting, this is expected to occur within 10 hours after the initiating event. With early containment venting, this is expected to occur at about 14 hours after the event.
- After the dc power is depleted, the RCIC injection flow could be shutoff or uncontrolled injection or remain as it's at the time dc depleted. This affects RPV status.
- MELCOR simulation estimates that after the loss of RCIC at 9.6 hour, the RPV water will reach the top of active fuel at 12.2 hours, and reach the minimum steam cooling water level (at about 1/3 of core high, the entry point into the Severe Accident Mitigation Guidelines (SAMGs)) at 12.5 hour, and core damage occurs at 13.9 hours.

Crew context

When the event occurred, the on-site staff is at the site administrative minimum shift staffing levels to respond to the two reactors simultaneously affected by the earthquake. It is assumed that there are no on-site personnel injured by the earthquake. Because of the blocked site accessibility, within the first six hours of the earthquake the on-site staff is the only available manpower to perform required actions. After 6 hours, the offsite personnel start to arrive onsite to provide needed manpower and the technical support center (TSC) and the operation support center (OSC) are established on site to support event mitigation. The offsite equipment is not available until 24 hours after the event.

Restoring ac power was one of the top immediate priorities of the operators. Once the shift supervisor determined that the ac power cannot be restored within one hour, an ELAP event is declared. The ELAP declaration led to the decision to deploy FLEX equipment.

The operator's main priority in this event is to maintain core cooling and to bring the reactor to a safe steady state. Because the control rods are automatically fully inserted after the earthquake, the core is sub-critical. The core cooling is only maintained by RCIC. The operator has an urgency to protect reliable RCIC operation, and in the meantime, establish

an additional mechanism to cool the core. The portable FLEX pump is the reasonable choice. Actions to prolong RCIC operation include shedding the dc load (RCIC is likely to trip once the essential dc load is lost), and venting the containment to slow torus heat up. The operator will principally follow the 100°F/hr rate to control the Safety Relief Valves (SRVs) to depressurize the RPV to between 200 and 400 psig. The RPV at this pressure range can generate enough steam to drive the RCIC pump and in case the RCIC fails, the FLEX pumps have enough pump head to pump water into the RPV.

During the first six hours, small teams are formed to perform various onsite tasks. In some situations, the team is led by experienced individuals and is supported by non-experienced individuals.

When performing containment venting and torus makeup, the operators will monitor the status of the heat capacity temperature limit (HCTL) and pressure suppression pressure (PSP). The HCTL indicates whether the torus has the sufficient capacity to absorb the heat dumped from the RPV. If the HCTL cannot be maintained, an emergency blowdown to depressurize RPV is required.

Because of the low margin of having sufficient manpower to perform the needed tasks within the first six hours, other plant staff were trained to perform or support certain FLEX strategies. A staffing analysis was performed to predetermine that the minimum onsite staff is sufficient to arrange the manpower with the needed skillsets to complete all key tasks. Because most of the onsite tasks are performed by teams, the plant staff are likely to work with individuals that are not normally in their group.

The main procedure used in this event include:

- RPV control procedure
- Containment control procedure
- SE-11: LOOP/SBO/ELAP procedure

Task context

The following are the operators' main tasks:

- Initial dc load shed to prolong the essential batteries' availability. This is a time critical task.
- Deep dc load shed to prolong further the essential batteries. This is a time critical task.
- Trip HPCI: RCIC and HPCI provide the same function in the ELAP event. Tripping the HPCI prolongs batteries for RCIC operation. Note: typically on BWRs, HPCI and RCIC are on opposite division batteries. In order to take advantage of a second battery, a manual circuit breaker cross-connection would have to be made.
- Use portable generator to re-charge the batteries to extend dc power availability: The decision to deploy the portable generator is when an ELAP is declared. This is a time critical task.
- Defeat RCIC high temperature isolation signal: This is a step of the LOOP procedure.
- Remove debris on the FLEX equipment transportation route and staging locations.
- Use portable pump to inject into RPV, torus, and SFP.

- Connect nitrogen bottles to SRVs to depressurize the RPV.
- Maintain RPV pressure between 200 and 400 psig to provide sufficient steam to drive RCIC turbine and, in case RCIC fails, the RPV will be depressurized to allow the use of portable (FLEX) pumps to inject water into RPV.
- Early vent the containment to maintain torus temperature below 230 °F: The exhaust steam of the RCIC turbine is dumped to the torus. Computer simulation indicates that the operator would vent the containment at 4.8 hours after the initiating event. With the containment venting, the torus temperature reaches 230 °F at 11.7 hours based on simulation.
- Open the RCIC room door to limit RCIC room heat up.
- The operators have to manually control RCIC injection rate to prevent the RPV water level from reaching the steam line. Without dc power, the RPV water level indication is not available. The operators have to go to the RCIC room to open steam valves to run the RCIC pump. It is expected that, in this situation, the operators are likely to have the steam valve fully open for maximum RCIC injection instead of manually control the flow rate.
- Manually transfer suction source from the Condensate Storage Tank (CST) to the torus if the automatic swap did not occur.

The baseline scenario timeline. The following information is based on [ML15245A364]

Initial condition:

- A plant site with two BWRs; Mark 1 containment in a dual reactor site with a common SFP for two reactors.
- Both reactors are at full power operation.
- Plant staffing is at the minimum emergency operation level.

Initiating event:

- A beyond design basis (BDB) earthquake caused an event of extended loss of ac power (ELAP) and the loss of ultimate heat sink (LUHS) due to failure of the downstream dam.

Boundary condition:

- The earthquake cause site-wide damage but the seismic class robust structures remain intact.
- No personnel injury. All onsite personnel are able to respond to the event.
- No site access is available within the first six hours following the earthquake.
- No concurrent major event, e.g., security, large fire, and external flooding.
- More detailed boundary conditions can be found in NEI 12-06 [ML].
- The main earthquake lasts for five minutes. No human action is performed within the first five minutes of the event.

Time (hh:mm)	**P:** Plant Responses **H:** Human Responses **N:** Notes

	I: Information
00:00	**P:** An extended loss ac power (ELAP) event and a loss of ultimate heatsink (LUHS) event due to a beyond design basis earthquake. **N:** Assume the main ground motion lasts for five minutes.
00:00+	**P:** Reactor Scrammed & Turbine tripped **P:** HPCI and RCIC start automatically on -48 inch signal. **N**: HPCI/RCIC actuation is an approximation – depending on how the event is initiated, RCIC could start automatically or be manually started by the operator. **I**: Alarm panels show overwhelmed alarms.
00:05	**H(MCR):** Enter RPV control procedure (based on reactor scram) **H(MCR):** Enter SE-11 "LOOP/SBO/ELAP procedure" based on no offsite power and no EDG loaded. **H(RO):** Shutdown HPCI **H(RO):** Call the onsite operators to report to the MCR **N:** Because no indication of a LOCA event, as long as RCIC is in service, HPCI operation is not required. Shutdown HPCI to conserve dc power.
00:15	**H(MCR):** Distribute master keys in MCR to onsite operators **H(EO2&3):** Locally start the EDGs per procedure X, attachment B (T_{action} = 45 min.). **H(EO1):** Shed dc load per SE-11, Att. T (T_{action} = 45 min.) **I:** Without shedding dc load, the batteries is expected to last for two hours. With the dc load shed, the battery is expected to last for five hours. **H(SM):** declared a site emergency based on **MS1 "**Loss of all Off-Site and all On-Site AC power to emergency busses for 15 minutes or longer". **H(SM):** mobilize the emergency response organization **N:** The dc load shed is performed at the cable spreading room, reactor building and turbine building. **N:** Backup N_2 cylinders are in the reactor building
00:20	**H(RO):** Open SRVs to cooldown and depressurize RPV. Reduce pressure to 500 psi, then 100°F/hr rate to between 200 and 300 psi. (2 hr)
00:30	**H(SSD2):** Commence opening RCIC/HPCI room doors per SE-11 Att.U.
01:00	**H(SM)**: Declare a general emergency based on **MG1 "**Prolonged loss of all Off-Site power all On-Site AC power to emergency busses" **H(SS):** Enter ELAP procedure due to no ac power is expected to be restored within 1 hour after the ELAP. **H(EO1):** Commence deep dc load she per FSG-012 ELAP DC Load Shed (T_{action} = 30 min.). **I:** With deep dc load shed, the batteries are expected to last for seven hours; otherwise, only last for five hours. **H(RP):** Establish backup N_2 per FSG-044 (T_{action} = 30 min.) **H(EO 2&3):** Dispatched to the FLEX building to commence debris removal and deploy FLEX equipment **H(SSD1):** Commenced to defeat RCIC trips and isolation (FSG-043)

	H(SSD2): Commenced antenna deployment and opening hatches and doors (FSG-020, FSG-033). **I:** The antenna allows the use of radio in the plant. **H(RO):** Commenced containment venting with tours pressure greater than 2 psig.
01:30	**H(EO1):** Completed dc load shed.
04:00	**H(RO2&):** Completed deployment of portable fans to supply cooling air flow to the RCIC rooms per FSG-042.
05:00	**H(EO1):** Commenced battery room venting per FSG-031.
05:30	**H(FBL&2):** Completed installation of SFP hoses on refuel floor per FSG-042.
05:45	**H(FB1):** Commenced control room venting per FSG-030.
06:00	**H(EO2):** Commenced deployment of portable pump that allows for makeup to the RPV, torus, and SFP. **I:** The staffing analysis shows that the task is performed by seven skilled staff and assisted by four non-skilled staff to transport hoses and pumps. **I:** There are a few pre-specified portable pump staging location. The first option is outside the reactor building. The pump take suction from the emergency cooling tower (a seismic class I structure and close to the reactor building) and discharge to the RHR. From the RHR, the water can be manually directed to RPV, SFP, or torus.
07:00	**H(EO3):** Portable generator is providing power to the safety related 480 VAC.
12:00	**H(RP):** Commenced makeup to SFP from FLEX Pump based on lowing SFP level.
24:00	**I:** Initial equipment from the regional resource center becomes available.
30:00	**H(EO1):** Commenced injection into torus.
24:00 – 72:00	**H(Crew):** Continue to maintain critical functions of core cooling (via RCIC), containment (via hardened vent opening and FLEX pump injection to torus), and SFP cooling (FLEX pump injection to SFP).

Operating Experience [the National Diet of Japan "The official report of executive summary, The Fukushima Nuclear Accident Independent Investigation Commission]: On March 11, 2011, the Great East Japan Earthquake triggered an extremely severe nuclear accident at the Fukushima Daiichi Nuclear Power Plant (NPP), owned and operated by the Tokyo Electric Power Company (TEPCO). When the earthquake occurred, Units 1, 2, and 3 of the Fukushima Daiichi plant were in at-power operation; and Units 4 to 6 were undergoing periodic inspections. The emergency shut-down feature, or SCRAM, went into operation at Units 1, 2 and 3 immediately after the commencement of the seismic activity. The seismic event caused a loss of the offsite power to the Daiichi NPP. The emergency diesel generators (EDGs) automatically started as designed. The tsunami caused by the earthquake flooded and totally destroyed the emergency diesel generators, the seawater cooling pumps, the electric wiring system and the DC power supply for Units 1, 2 and 4, resulting in loss of all power - except for an external supply to Unit 6 from an air-cooled emergency diesel generator at about 50 minutes after the earthquake. In short, Units 1, 2 and 4 lost all power; Unit 3 lost all AC power, and later lost DC power before dawn of March 13, 2011. Unit 5 lost all AC power.

The tsunami did not damage only the power supply. The tsunami also destroyed or washed away vehicles, heavy machinery, oil tanks, and gravel. It destroyed buildings, equipment installations and other machinery. Seawater from the tsunami inundated the entire building area and even reached the extremely high pressure operating sections of Units 3 and 4, and a supplemental operation common facility (Common Pool Building). After the water retreated, debris from the flooding was scattered all over the plant site, hindering movement. Manhole and ditch covers had disappeared, leaving gaping holes in the ground. In addition, the earthquake lifted, sank, and collapsed building interiors and pathways, and access to and within the plant site became extremely difficult. Recovery tasks were further interrupted as workers reacted to the intermittent and significant aftershocks and tsunami. The loss of electricity resulted in the sudden loss of monitoring equipment such as scales, meters and the control functions in the central control room. Lighting and communications were also affected. The decisions and responses to the accident had to be made on the spot by operational staff at the site, absent valid tools and manuals.

Outcome of Step 2 - HFE identification, definition, and feasibility assessment

The baseline event sequence and deviation event sequences through "What-If" questions

Based on the important equipment and human action identified in the baseline scenario, with interaction with PRA analyst, the following are the what-if questions:

- What-if the DC power failed at
  - t = 0 hr (failed by the earthquake)
  - t = 2 hr (due to operators failing to shed the dc load)
  - t = 5 hr (due to operators failing to deep shed dc load)
  - t = 7 hr (due to operators failing to use the portable generators to charge the essential batteries before the batteries deplete.
- What-if the RCIC failed at
  - t = 0 (failed by the earthquake)
  - When the dc power is not available
  - When the torus temperature reaches 230 °F
- What-if the operator failed to depressurize the RPV (RPV remains at high pressure)?
  - When the dc power is not available
  - When there is not enough pneumatic pressure to operate the SRVs.
- What-if the operator over depressurize the RPV so there is not enough steam to drive the RCIC pump?
- What-if the RPV was unexpectedly depressurized due to hardware failure, e.g., stuck open SRVs?
- What-if the operator vented containment at a different time?

- When the containment pressure is 2 psig. This is the earliest time the procedure allows venting the containment even though the operator can decide not to vent.
- When the containment is between 10 and 15 psig. This is an operational estimate that operators are most likely to vent the containment at this point.
- Did not vent the containment
- Vent the dry well because the reactor building debris precludes the accessibility to perform wetwell vent.

- What-if the operator did not close the containment vent valve when the core damage occurred? The expectation is the containment vent valve will be closed after core damage.
- What-if the operator failed to use the portable pump to cool the core? The expectation is that the portable pump is ready to cool the core five hours after the decision is made.

HFEs and definition

HFE 1 - Use portable pump to feed the RPV

Definition:

Condition: The RPV pressure is controlled between 200 – 400 psig. The operator is sensing the RCIC is losing its function because the torus temperature is approaching to 230°F so the operator decided to use the portable pump to inject into RPV.

Key operator actions:

- Setup the potable pump and align the injection path (See Note 1 for detail). This includes remove debris from the equipment transportation route. (See Note 2 for detail)
- Start the pump and monitor the pump status
- Depressurize RPV completely (from between 200 and 400 psig) to allow water injection

Notes:

1. The portable pump is staged outside of the Reactor Building (about 100 feet away from the reactor building). The pump takes suction from a 4" stortz penetration of the emergency cooling tower, which is a seismically robust structure. Hardened hoses are used for suction. It is about 50 feet to the water source. The operator has to use a 2.5 inch fire hose to connect the pump discharge to a RHR connection inside the reactor building. The length of the hose connection is about 300 feet.
2. The decision to deploy the portable pump is made at one hour after the initiating event. The decision to use the portable pump to inject into the RPV is assumed to be made at nine hours after the initiating event (the torus temperature reaching 230°F is calculated soon before 10 hours after the initiating event). The portable pump must be ready for RPV injection when the operators make the decision for portable pump injection. The needed actions to inject water from the portable pump to the RPV is to

depressurize the RPV, open the RHR system valve connected to the portable pump, and operate manual valves to direct the flow into the RPV.

Success criteria:

- The operator decided to deploy the portable pump one hour after the earthquake.
- The portable pump is setup, aligned, and is running ready to inject water into RPV. At this point, the only needed action to inject into the RPV is to manually open the RHR local valve connected by fire hose to the portable pump assuming the RPV is depressurized (see the next bullet).
- The RPV is successfully depressurized completely from between 200 and 400 psig.

Special equipment: Portable pump, hoses, and communication devices. The equipment is available.

Staffing requirement: Four people to remove debris on the equipment transportation route; three people to transport and set up the portable pump and hoses for each reactor. The site has sufficient manpower and skillset to perform the task.

HFE Feasibility analysis

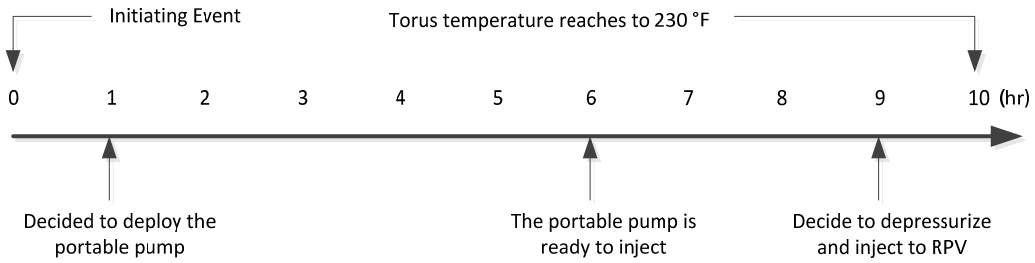
- Sufficient time: Yes
    - Available time for action is eight hours (assuming the decision to deploy the portable pump is made at one hour after the initiating event).
    - The required action time (including removing debris) is five hours.
- Credible cue(s): Yes, based upon the cue, the Shift Supervisor expected the ac power cannot be restored within an hour.
- Procedures / guidance / instructions and training: Yes
    - ELAP procedure for making the portable pump deployment decision
    - FSG-002 for debris removal
    - FSG-040 for aligning the portable pump from the emergency cooling tower to the RHR.
- Sufficient manpower and skills: Yes
- Location accessibility: Yes
- Equipment (HSI of pre-positioned systems / equipment, on-transport equipment, portable equipment, and communication devices) operability and resources: Yes

Sufficient time –

Time Available: 9 hours.

Outcome of Step 3: Task analysis and time uncertainty

CRD - representing the expected crew response paths along with the timeline of critical responses



Critical tasks

Critical task 1 - Decide to deploy the portable pump

Critical task 2 – setup the portable pump to inject into RPV

Time uncertainties and their contribution to HEP

Estimation of Time available:

- Standard Distribution
- The mean is 9 hours
- The standard deviation is 20 minutes.

Estimation of time needed:

- Standard Distribution
- The mean is 6 hours
- The standard deviation is 30 minutes.

Estimation of HEP resulted from time uncertainty

Outcome of Step 5: Identification of CFM and estimation of HEP

Critical task 1: Decide to deploy the portable pump

Applicable cognitive functions

Detection – The detection includes detecting loss of offsite power and loss of EDGs. Both have vivid indications in the MCR. This led the operators to transfer to the SBO procedure.

Understanding – The shift supervisor understands that the ac power is not expected to be restored within one hour based on the SBO procedure instruction. This led the operator transfer to the ELAP procedure. Once the SS received confident answers from the ROs and the regional transmission operators' assessment on restoring ac power, the understanding of the situation is straightforward.

Decision-making – The ELAP procedure directs the operation of the portable pump. With a correct understanding, the decision is straightforward.

Applicable CFMs

Detecting: The potential SFMs are:

- D5-1 *Incorrectly interpret, organize or classify information (e.g., incorrectly recognize the trend of a parameter).* ***Explanation:*** *The EO incorrectly assessed that the EDGs can be restored within an hour.*
- D6-1 *Detected cues not retained or incorrectly retained (mark wrong items, wrong recording, wrong data entry).* ***Explanation:*** *The SS was unable to obtain a clear answer from the regional electric transmission operator that the offsite power can be restored within one hour.*

When the time is close to one hour and the SS has not received positive, confident indications from the EOs and the region transmission operators, the SS is expected to follow SBO instruction to declare an ELAP event.

Applicable PIFs

BHFE:

- Criteria are ambiguous. **Explanation:** the EOs in checking the EDGs and the region transmission operator cannot definitely state whether or not the electricity can be restored within one hour. (BHEP = 1E-4 ~ 5E-1)

Modification Factors:

- Unfamiliar scenario (0.5 ~ 2). **Explanation:** The ROs and transmission operators have not experience BDB earthquake effects on EDGs and the electricity network.
- PROLONGED ATTENTION: Information changes over time and requires sustained attention (> 10 minutes) (0.5 ~ 2). **Explanation:** The SS is eager to have the information as soon as possible.

Critical task 2: setup and align the portable pump to inject into the RPV

Applicable cognitive functions

Action execution – Led by the trained equipment operators, there is a team effort to setup and align the portable pump. The MCR operators open SRVs to depressurize the RPV. An equipment operator locally opens an RHR valve for the portable pump flow to inject into the RPV through the RHR system piping.

Applicable CFMs

- E3-1 *Delayed implementation.* ***Explanation:*** *The action will most likely be initiated but the action may not be implemented in time for various reasons.*

Assessment of PIFs

BHEP:

- Location accessibility (travel paths, security barriers, and sustained habituation of worksite) (0.001 ~ 0.1) **Explanation:** the debris and gate in the travel route may prevent the equipment from being deployed in time.
- Criteria for actions are infrequently trained or operators rarely perform the actions (0.01 ~ 0.5) **Explanation:** Except for the initial training, the equipment operators are trained on operating the equipment during surveillance tests. Hands-on training on the whole setup and alignment process is infrequently if not never performed. Nevertheless, the actions are straightforward and the connection locations are familiar to the equipment operators.

Modification Factors:

- Frequent or persistent interruption/distraction (0.1 ~ 0.5). **Explanation:** The actions take about five hours. After shocks are expected during the five hours that could interrupt the portable equipment deployment.
- Unfamiliar, distributed, or unstable operational teams (0.1 ~ 1). **Explanation:** Two work groups are needed to deploy the portable equipment: debris removal group and the portable pump and hose transport and setup group. Each work group includes several workers temporarily formed as a team based on the limited manpower available on site.

Appendix E: Insights on PIF interaction from cognitive literature

Most human failure events modeled in HRAs involve more than one PIF. HRA methods treat the effects of combination of PIFs in ways:

- *Holistic estimation* – Experts estimate the probability of a human failure event or a failure mode for a given set of PIFs (also referred as to scenario context) considering but not explicitly modeling the combination of PIFs.
- *Multiplication* – The HEP is the product of a baseline HEP with multipliers associated with individual PIFs. (This is the approach used by most current HRA methods.)

To determine if we could find a cognitive basis for the quantitative treatment of PIF combinations, we searched the cognitive experiment literature for those studies that examined the individual and combined effects of two or more PIF indicators. We extracted the error rate data in the following format:

R_0: Baseline error rate when both indicators are low or absent
Ra: Error rate when indicator A is high and B is low
R_b: Error rate when indicator A is low and B is high
R_{ab}: Error rate when indicators A and B are high

We then calculated the weights for the indicators:

$$W_a = R_a/R_0$$
$$W_b = R_b/R_0$$
$$W_{ab} = R_{ab}/R_0$$

If the combined effect is multiplicative, then

$$W_{ab} = W_a * W_b$$

If the combined effect is additive, then the increased error rate of combined PIF indicators from the baseline condition should be equal to sum of the increased error rates of the individual PIF indicators, i.e.,

$$(R_a - R_0) + (R_b - R_0) = R_{ab} - R_0$$

We applied the above analysis to 23 sets of data from the literature. One example is the study performed by Patten et al (2006) that explored the effect of task complexity and experience on driver performance. Table 1 shows the error rates for two PIF indicators: low experience vs high experience, and low complexity (simple) vs. high complexity tasks:

Table 1: Mean error rate (% incorrect) in Patten et al study

	High experience	Low experience
Low complexity	12	21
High complexity	25	32

Here,

$$W_a = 21/12 = 1.75$$
$$W_b = 25/12 = 2.2$$
$$W_{ab} = 32/12 = 2.67$$

Using the multiplication rule, $W_a * W_b = 3.85$, which is higher than W_{ab}. Using the additive rule, $(R_a - R_0) + (R_b - R_0) = 22\%$ and $(R_{ab} - R_0) = 20\%$; the sum of the individual effects is close to the combined effect.

Therefore, the additive rule appears to quantify the combined effect better than the multiplicative rule for this set of data.

Table 2 lists several other examples. The columns from left to right are for references, task type, PIF indicators, and error rates (R_0, R_a, R_b, R_{ab}) and calculated weights (W_a, W_b, W_{ab}).

Table 2: Error rates for individual and combined PIF indicators

Ref.	Task	PIF indicators	Error rates
Lee[15]	Driving simulation	A: Warning time B: Driving speed	R (1, 22, 3, 31) W (22, 3, 31)
Cummings[17]	Air traffic control simulation	A: HSI format B: Task load	R (4,8,12,20) W (2, 3, 5)
Colquloun[24]	Detection	A: Signal saliency B: Criterion	R (25,45, 45,70) W (1.8,1.8, 2.8)
Strayer[25]	Driving simulation	A: dual-task B: Distraction	R (2.5,4,5, 6) W(1.8,2,2.4)
Xing[26]	Color use tests	A: Complexity B: Color vision deficiency	R (2,4,32,34) W(2,16,17)

For all these examples, $W_a * W_b$ is significantly greater than W_{ab}, suggesting that the data do not support the multiplicative rule. On the other hand, the additive rule seems to fit the data well.

An exception to the trend shown by the examples in Table 2 is the study of the effect of message complexity on pilot communication errors by Prinzo et al (2007). Table 3 shows the error rates for low vs. high complexity and task difficulty (Departure vs. Approach).

Table 3: Mean error rate (% incorrect) in Prinzo et al study

	Departure	Approach
Low complexity	4	5
High	8	20

complexity		

Here,

$$W_a = 5/4 = 1.25$$
$$W_b = 8/4 = 2$$
$$W_{ab} = 20/4 = 5$$

Per the multiplication rule: $W_a * W_b = 2.5$, which is less than W_{ab}. Per the additive rule: $(R_a - R_0) + (R_b - R_0) = 5\%$, whereas $(R_{ab} - R_0) = 16\%$. This appears to be an unusual case where neither multiplicative nor additive rule works. The reason may that, in fact, both indicators challenge the same cognitive limit, the capacity of working memory. When both indicators are high, the working memory load exceeds the capacity limit, leading to the high error rate.

Since we did not systematically mine the experimental data nor perform a meta-data analysis, we do not attempt to draw strong conclusions from the limited sample of the literature. We only make several observations from the 23 sets of data we reviewed:

1. The multiplicative rule tends to over-estimate the combined effect of PIF indicators on error rates, while the additive rule can roughly interpret the results.
2. The individual and combined weights (W_a, W_b, W_{ab}) of PIF indicators are typically in the range of 1-5 and rarely exceed a value of 10.
3. The individual and combined effects of PIF indicators can behave differently if the indicators show a demand on cognitive resources that exceeds the cognitive limits.

REFERENCES