NUREG-**, Vol. 1**

Collaboration between the NRC and EPRI

An Integrated Human Event Analysis System (IDHEAS) for NPP Internal At-Power Application

Draft Report: 2/19/2016

Prepared by:

Jing Xing[1], Gareth Parry[2], Mary, Presley[3],
John Forester[4], Stacey Hendrickson[5], Vinh Dang[6]

[1]U.S. Nuclear Regulatory Commission
[2]Jensen Hughes
[3]Electric Power Research Institute
[4]Idaho National Laboratory
[5]Sandia National Laboratories
[6]Paul Scherrer Institute

NRC project managers: Erasmia Lois and Jing Xing

EPRI project managers: Stuart Lewis and Mary Presley

Contributors to Report

The authors would like to thank the following people who made invaluable contributions to the report (in alphabetical order):

Dennis Bley, Buttonwood Consulting

Ronald Boring, Idaho National Laboratory

James Chang, US Nuclear Regulatory Commission

Katrina Groth, Sandia National Laboratories

Dana Kelly, Idaho National Laboratory

Stewart Lewis, Electric Power Research Institute

Huafei (Harry) Liao, Sandia National Laboratories

Erasmia Lois, US Nuclear Regulatory Commission

Ali Mosleh, University of Maryland (now UCLA)

Johanna Oxstrand, Idaho National Laboratory

Marty Sattison, Idaho National Laboratory

Song-Hua Shen, US Nuclear Regulatory Commission

Nathan Siu, US Nuclear Regulatory Commission

Susan Stevens-Adams, Sandia National Laboratories

April Whaley, Idaho National Laboratory

Table of Contents

1 Introduction 1
1.1 Background and Objectives 1
1.2 Approach for Development 2
1.3 Assumptions underlying the use of the method 3
1.4 HRA Process and Report Structure 4
1.5 Continuous Development and Improvement of HRA 5
1.6 References 6
2 An Overview of IDHEAS 9
2.1 The HRA Process and the Elements of IDHEAS 10
2.2 Scenario analysis 11
2.2.1 Document initial condition, initiating event, and boundary condition 11
2.2.2 Develop the baseline scenario 12
2.2.3 Perform context analysis 12
2.3 Identification and Definition of HFEs 13
2.3.1 Identification of HFEs 13
2.3.2 HFE Definition 15
2.3.3 Initial Assessment of Feasibility 16
2.3.4 Time uncertainty analysis 17
2.4 Task Analysis and the Development of Crew Response Diagrams (CRDs) 17
2.5 Implementation of the Quantification Model 18
2.6 Integration – Results Review, Documentation, Dependency Analysis and Recovery Actions 19
2.7 References 19
3 HFE Feasibility Assessment and Time Uncertainty Analysis 20
3.1 Feasibility Assessment Criteria 20
3.1.1 Sufficient Time to Complete the Tasks 21
3.1.2 Sufficient Manpower 21
3.1.3 Cues Available 21
3.1.4 Procedures and Training 22
3.1.5 Accessible Location 22
3.1.6 Availability of Equipment Required for Critical Tasks 23
3.1.7 Operable Relevant Components 23
3.2 Guidance on Time Estimation Addressing Uncertainty 23
3.2.1 Definitions 24
3.2.2 Guidance of estimating the distribution of time needed 25

3.2.3 Bias factors in time estimation 27
3.3 Consideration of Timing Results Before Use of the IDHEAS DTs 29
3.3.1 Maximum Time Requirement 30
3.3.2 Time Margin 30
3.4 Calculation of HEP for time critical responses 31
3.5 References 32
4 Task Analysis and Development of Crew Response Diagrams 33
4.1 Introduction 33
4.2 Task Analysis and Associated Timeline 34
4.2.1 Overview 34
4.2.2 Stage1. Characterization of the Expected Procedural Success Path 37
4.2.3 Stage 2. Identification and Detailed Definition of Critical Tasks 39
4.2.4 Stage 3. Identification of Potential Recovery Opportunities 42
4.3 Analysis of the CRD 44
4.4 Example Demonstration of Task Analysis and Development of CRD 44
4.4.1 Definition of the HFE Used in the Example 44
4.4.2 Task Analysis Stage 1 Result – Characterization of the Expected Success Path. 45
4.4.3 Task Analysis Stage 2 Result – Identification and Detailed Definition of Critical Tasks 49
4.4.4 Task Analysis Stage 3 Result – Identification of Recovery Potential 52
4.4.5 Timeline for the Example HFE 55
4.5 References 56
5 HRA Quantification Model 57
5.1 HRA Quantification Model – Concept 57
5.1.1 Crew Failure Modes (CFMs) 57
5.1.2 PIFs and Development of Decision Trees as the Basis for HEP Quantification 61
5.1.3 Workload factors 63
5.1.4 Estimation of HEPs of DT paths 64
5.2 CFMs and DTs for internal at-power events 66
5.2.1 AR: Key Alarm Not Attended To 66
5.2.2 SA-1: Data Misleading or Not Available 70
5.2.3 SA-2: Wrong Data Source Attended to 75
5.2.4 SA-3: Critical Data Misperceived 78
5.2.5 SA-4: Critical Data Dismissed/Discounted 82
5.2.6 SA-5: Premature Termination of Critical Data Collection 86
5.2.7 RP-1: Misinterpret Procedure 90
5.2.8 RP-2: Choose Inappropriate Strategy 94

5.2.9 E-1: Delay Implementation 97
5.2.10 E-2: Critical Data Not Checked with Appropriate Frequency 101
5.2.11 Action CFMs: Fail to Execute Action / Fail to Correctly Execute Response 105
5.2.12 AP-1: Misread or Skip Step in Procedure 118
5.2.13 C-1: Critical Data Miscommunicated 121
5.3 Treatment of Recovery 124
5.4 References 128
6 Implementation of the IDHEAS Method – HEP Estimation 129
6.1 Introduction 129
6.2 Implementation of the Quantification Model 129
6.2.1 Step 1: Organize the qualitative analyses associated with characterizing the failure paths on the CRD 130
6.2.2 Step 2: Selection of CFMs for Each CRD Failure Path 132
6.2.3 Selection of Path through the Decision Trees and Assignment of HEPs 133
6.2.4 Calculation of the HEP for the HFE 133
6.3 Example Quantification of an HFE 134
6.3.1 Inputs to Quantification –HFE Definition and Task Analysis 134
6.3.2 Identification of the CFMs Applicable to the HFE 136
6.3.3 Application of the DTs to Quantify Crew Failure Paths 138
6.3.4 Calculation of the Combined HEP for the HFE 142
7 Model Integration 143
7.1 Results Review and Reasonableness Check 143
7.1.1 Iteration with Accident Sequence Development 144
7.1.2 Documentation 144
7.2 Recovery Analysis 145
7.3 Dependency Analysis 145
7.3.1 Dependency Model 146
7.4 Uncertainty Analysis 149
7.5 References 151
8 Epilogue 153
8.1 Outstanding Issues 153
8.2 Development of an improved approach to dependency analysis using the characteristics of the IDHEAS method 154
8.2.1 Dependencies between HFEs 154
8.2.2 Dependencies within HFEs 155
Appendix A. Example Application of IDHEAS Method 1
A.1 Scenario 1: Total Loss of Feed Water (LOFW) with Misleading Indicator 1

A.1.1 PRA Scenario Description, Expected Operator Response and HFE Definition 1
A.1.2 Crew Response Diagram (CRD) and Task Analysis 2
A.1.3 Timeline 8
A.1.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees (DTs) 10
A.2 Scenario 2: Loss of RCP Sealwater 17
A.2.1 PRA Scenario Description, Expected Operator Response and HFE Definition 17
A.2.2 Crew Response Diagram (CRD) and Task Analysis 19
A.2.3 Timeline 22
A.2.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees (DTs) 24
A.2.5 Summary of Analysis 31
A.3 Scenario 3 – Fail to Cooldown and Depressurize Following a Small LOCA 34
A.3.1 PRA Scenario Description, Expected Operator Response and HFE Definition 34
A.3.2 Crew Response Diagram (CRD) and Task Analysis 35
A.3.3 Timeline 39
A.3.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees (DTs) 40
A.3.5 Summary of Analysis 44
Appendix B. Lessons Learned from Existing HRA Methods and Activities and a Detailed Description of the Approach used for IDHEAS 1
B.1 Lessons Learned from Existing HRA Methods and Activities 1
B.1.1 HRA Good Practices 1
B.1.1.1 Strengths in Current Methods 1
B.1.1.2 Limitations in HRA Process 2
B.1.2 Lessons Learned from NUREG-1852 and NUREG-1921 3
B.1.3 Findings from HRA Empirical Studies 3
B.2 Approach 5
B.2.1 Integration of the Strengths of Existing Methods 5
B.2.2 Psychological Literature Review 6
B.2.3 Development of IDHEAS- the qualitative analysis structure and quantification model 7
B.2.3.1 The qualitative analysis structure 7
B.2.3.2 HFE quantification 8
B.3 References 10
Appendix C. Selection of Proximate Causes (PCs), Cognitive Mechanisms, and Performance Influencing Factors (PIFs) 1
C.1 Mapping of PCs, cognitive mechanisms, and PIFs for every CFM 1
C.1.1 Plant Status Assessment Phase 1
C.1.1.1 AR: Key Alarm Not Attended To 2
C.1.1.2 SA-2: Wrong Data Source Attended to 4

C.1.1.3 SA-3: Critical Data Misperceived 5
C.1.1.4 SA-4: Critical Data Dismissed/Discounted 6
C.1.1.5 SA-5: Premature Termination of Critical Data Collection 8
C.1.2 Response Planning Phase 10
C.1.2.1 RP-1: Misinterpret Procedure 10
C.1.2.2 RP-2: Choose Inappropriate Strategy 11
C.1.3 Action/Execution Phase 12
C.1.3.1 E-1: Delay Implementation 13
C.1.3.2 E-2: Critical Data Not Checked with Appropriate Frequency 14
C.1.3.3 E-3: Fail to Initiate Execution 16
C.1.3.4 Fail to Correctly Execute Response (E-4: Simple and E-5: Complex) 17
C.1.4 CFMs that Represent Multiple Phases 18
C.1.4.1 AP-1: Misread or Skip Step in Procedure 19
C.1.4.1 C-1: Critical Data Miscommunicated 20
C.2 Cognitive mechanisms and PIFs 22
Appendix D. Expert Judgment of HEP Distributions for IDHEAS Decision Trees 1
D.2 Objective of the Expert Elicitation (EE) 1
D.3 The SSHAC method for obtaining expert judgment 1
D.3.1 Selection of SSHAC Level 2
D.3.2 Project Organizational Structure 2
D.4 Process for EE 3
D.4.1 Preparation 3
D.4.2 Workshop 1 4
D.4.3 Workshop 2 & 3 5
D.4.4 Integration and interpolation ..... **Error! Bookmark not defined.**
D.5 Summary Consensus Distributions 6
D.5.2 Findings and Conclusions 6

Executive Summary

This report presents the Integrated Human Event Analysis System (IDHEAS) method for human performance in internal at-power operation developed for addressing the staff requirements memorandum SRM-M061020 on HRA Model Differences. We will also develop an IDHEAS User's Manual that provides concise step-by-step guidance for using this method in analyzing proceduralized human events for an internal events at-power PRA. The details of the cognitive basis for IDHEAS were described in a separate report (NUREG - 2114). Also, a separate report developed by the NRC staff describes the IDHEAS General Methodology for human performance in NPP-related operations. This report includes the following chapters:

Chapter 1*, Introduction*, consists of background of the work, the scope of the work, general approach, overview of the method, and perspectives on how this work is addressing various NRC needs for HRA.

Chapter 2, *An Overview of IDHEAS*, describes at a high level, the IDHEAS process which begins with understanding of the PRA scenarios and collecting information from PRA for HRA analysis, identifying and defining HFEs in the HRA framework, and the performance of a task analysis and implementation of the quantification model. The chapter also provides guidance for an initial HFE feasibility analysis.

Chapter 3, *HFE Feasibility Assessment and Time Uncertainty Analysis*, describes the process to determine the feasibility of an action, guidance for evaluating timing elements necessary for the analysis, and introduces a new approach for estimating the HEPs for time-critical actions.

Chapter 4, *Task Analysis and Development of Crew Response Trees*, provides an overview of and guidance for the task analysis of the HFE and guidance for developing and using Crew Response Diagrams (CRDs) to identify critical tasks in an HFE. Also presented is an example development of a CRD.

Chapter 5, *HRA Quantification Model – Crew Failure Modes and Decision Trees,* provides a detailed quantification model focusing on analyzing the failure of the critical tasks, including the development as well as the outcomes of crew failure modes (CFMs) and decision-trees (DTs) for the failure modes. The chapter also provides guidance on how to determine the failure paths within a DT.

Chapter 6, Implementation of the IDHEAS method – *HEP Estimation,* describes a step-by-step process of estimating the HEP for an HFE using the qualitative analysis results and the quantification model. This chapter serves as a high-level user's manual for using IDHEAS to perform HRA.

Chapter 7, *Model Integration*, provides guidance for treatment of recovery analysis, treatment of dependencies between HFEs, and uncertainty analysis. The guidance adapts the state-of-practice in existing HRA methods. The chapter also presents an analysis of the existing practices of modeling dependencies and their limitations, and proposes new approaches for modeling dependencies using the IDHEAS framework.

Chapter 8, *Epilogue,* discusses issues that are outstanding and will be attended to in the next draft report following user testing and the development of the User's Guide.

Appendix A: *Example Applications of the IDHEAS Method*. This appendix presents three example HFEs that were evaluated using the IDHEAS methodology to demonstrate how the entire process fits together, including: documentation of the PRA Scenario, the expected operator response and the HFE definition, documentation of the analysis of the HFE in the form of a CRD and timeline, determining the applicable CFMs for each node and evaluating the corresponding DTs, and finally quantifying the total HEP and examining the risk insights.

Appendix B: *Lessons Learned from Existing HRA Methods and Activities and a Detailed Description of the Approach used for IDHEAS* provides background information that motivated the devleopement of this method as well as lessons learned from the study of existing methods and their applications.

Appendix C: *Selection of Proximate Causes (PCs), Cognitive Causes, and Performance Influencing Factors (PIFs)*. This Workshopescribes the mapping of crew failure modes to the macrocognitive functions, proximate causes and cognitive causes identified in the psychological literature review (NUREG-2114) and describes the selection of relevant PIFs used in the decision trees.

Appendix D: *Summary of Expert Elicitation to Obtain HEPs for IDHEAS Decision Tree Paths*. This appendix overviews the expert elicitation process and workshops held to develop the HEPs for use in the decision trees.

1 INTRODUCTION

1.1 Background and Objectives

Probabilistic risk assessment (PRA) results and insights are frequently used to support risk-informed regulatory decision making. The U. S. Nuclear Regulatory Commission (NRC) continues to improve the robustness of PRA, including human reliability analysis (HRA) through many activities (e.g., supporting and endorsing PRA standards developed by professional societies). Improving HRA has been a focus of the NRC since the publication of NRC's PRA policy statement [1]. A particular HRA issue is the variability of results from method-to-method and analyst-to-analyst. That is, the human error probability (HEP) for a particular human failure event (HFE) can vary significantly depending on the HRA model/method used and/or the analyst applying the method.

In a Staff Requirements Memorandum (SRM) (SRM-M061020) [2] to the Advisory Committee on Reactor Safeguards (ACRS), the Commission directed the ACRS to "work with the staff and external stakeholders to evaluate the different human reliability models 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 staff and representatives of the Electric Power Research Institute (EPRI) met with the ACRS in April 2007 and presented a plan for addressing SRM-M061020. The ACRS, in a letter to the Commission entitled *Human Reliability Analysis Models*, dated April 23, 2007 (ACRSR-2247) [3] stated that: "The staff should compare the NRC and EPRI models with respect to their basic assumptions and intended use. An evaluation of these assumptions and their supportive evidence should be performed." With a series of reviews (e.g., [4-6]), analyses, and discussion, the staff decided to develop a new HRA method that integrated the strengths of existing HRA methods and improved some key limitations in the HRA state of practices by incorporating the knowledge of human performance and cognitive psychology.

The Office of Nuclear Regulatory Research (RES) took the lead in addressing SRM-M061020. The ACRS has been providing inputs through periodic meetings. The work has been performed collaboratively with EPRI under a RES/EPRI Memorandum of Understanding (ADAMS: ML070740114 [7] and its update, ML100490657 [8]). EPRI's participation was motivated by a recognition that, although the methods currently employed by its members were serving needs for risk management and risk-informed applications well, those methods had not been substantively updated in more than 20 years and needed improvement in several areas. EPRI is interested in pursuing enhanced methods that can yield practical insights into human reliability and further improve reproducibility of the results.

To begin addressing SRM-M061020 [2], a detailed literature review was performed, including a review of current psychological research [9], existing HRA methods [10], results of the International HRA Benchmarking studies [4-5] and other HRA guidance [11-12]. In addition, the development team conducted discussions with NRC staff and external stakeholders regarding the HRA state-of-practices and needs. The conclusion was that each individual existing method had its own strengths, weaknesses, and specific application scope; therefore, the staff concluded that characteristics of several methods should be incorporated into a new integrated method to meet the SRM objective; the new method should incorporate the lessons learned from the International and US HRA empirical studies [4-6] and reviews of existing HRA methods and guidance, as well as the state-of-the-art knowledge of human errors from cognitive psychology research. The new method is referred to as an Integrated Human Event Analysis System (IDHEAS). IDHEAS is intended as a new HRA method firmly grounded in HRA technology and experience as well as the state-of-knowledge on Human Factors and Human Performance. This project has sought to achieve this goal by mining the current state-of-the-art knowledge, up-dating the theoretical basis for HRA, and building on existing technology and

experience. Knowledge and experience for achieving these goals comes not only from HRA applications and studies but also from the over 30 years of PRA experience that has shown how variability in other areas has been (and continues to be) addressed through the employment of causal logic models and development of rules and computer capability aiding stabilization of the technology.

Given the need to update the fundamental knowledge employed by HRA methods, the project first performed a comprehensive cognitive literature study to identify "direct linkages" of cognitive mechanisms to observed failures and to consolidate the information into a cognitive framework for HRA. The framework is constructed on macrocognitive functions, which 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 macrocognitive functions relevant to human performance in complex and dynamic domains can be characterized as: *Detecting*; *Understanding*; *Decision-making & Planning*; *Action Execution*; and *Teamwork*. IDHEAS is based on this cognitive framework.

Recognizing the needs for reducing method-to-method and analyst-to-analyst variability in HRA, the project took a strategic approach: 1) developing a cognitive basis framework, 2) from the cognitive basis framework, developing a general HRA methodology that can be adapted to any given HRA applications, including internal and external events, at-power and shutdown, NPP operation and non-NPP operations (such as fuels and materials handling, radioactive equipment use), and 3) from the general methodology, developing concise, application-specific HRA methods for given applications. With this strategy, the project so far has developed three products: a cognitive basis framework for human error analysis, IDHEAS for internal at-power events, developed as a joint effort between the NRC and EPRI, and a generic HRA methodology developed by the NRC staff, referred to as IDHEAS General Methodology (IDHEAS-G). This report describes IDHEAS for internal at-power operation. The objective was to develop an HRA method to reduce analyst-to-analyst variability and improve estimates of human error probabilities (HEPs) for internal at-power application because that comprises the majority of the HRA experience base and application. The method was aimed to be a stand-alone HRA method with the following characteristics:

1. Integrates the good features in HRA state-of-practice methods and incorporates the state of knowledge on human performance and cognitive psychology;
2. Is practical and straightforward to use;
3. Provides traceable and reproducible results.

For simplification, this method is referred to as IDHEAS in this report.

1.2 Approach for Development

The key features of IDHEAS for internal at-power application include the following:

1. The method focuses upon actions typical to at-power, internal events PRA and, in particular, on procedure driven actions. The assumption is that human actions modeled by the method are performed by crews trained on well-developed procedures in NPP control rooms.
2. IDHEAS was intended to address the estimation of the probabilities of human failure events (HFEs) that have been identified for inclusion in a plant PRA; the identification of HFEs was not a focus of its development.
3. IDHEAS consists of a qualitative analysis process that includes a detailed cognitive task analysis and a HEP quantification model for HFEs that are identified for inclusion in a PRA and defined at a functional level.

4. The qualitative analysis process and quantification model were developed with reference to internal at-power events; they may be applicable to other applications with reasonableness checking and modifications.
5. The method is intended to meet the ASME/ANS PRA Standard [13] as a detailed HRA method for analyzing risk-significant events

We recognize that the overall goal of reducing the inter-analyst variability is an ongoing endeavor. Even though the HRA method provides an approach, key concepts, "data," and tools (including language as well as analytical devices), it will still need to be exercised by analysts for different applications. The goal of this method at the present stage is to provide cohesive guidance for qualitative analysis and a concise quantification model specific for internal at-power operation to improve the quality of HRA predictions, particularly related to understanding crew responses and estimating HEPs.

However, it should be recognized that the present document should not be considered a user's guide. While the document does provide significant guidance for performing an HRA using IDHEAS and covers all the major aspects of performing an HRA, there remain areas (e.g., the development of crew response diagrams to support the qualitative analysis) where it is likely that additional guidance will be needed for efficient, effective, and consistent use of the method. In addition, there are other areas where guidance is provided, but the IDHEAS specific guidance has not yet been developed. For example, guidance for performing the requisite HRA dependency analysis is provided, but it is based on earlier approaches to treating dependency and does not capitalize on unique aspects of the IDHEAS framework (e.g., it is a causal model and dependency is a causal issue) that should lead to significant improvements in the ability to adequately address dependency (see Section 8.3 for a brief discussion of the expected advantages). Thus, additional work beyond that described in this document will be required to complete the planned methodology and develop a thorough user's guide.

1.3 Assumptions underlying the use of the method

The following assumptions are implicitly made for human failure events (HFEs) analyzed with IDHEAS for Internal at-power application:

- Operators trust and follow their procedures. Therefore, accident sequences are developed based on the expected procedure progression given the initiating event. Without this assumption bounding scenarios cannot be developed. One consequence of this is that, to some extent, errors of commission or deliberate violations of procedures are not modeled.
- The set of operating procedures (EOPs, AOPs, annunciator response procedures, system operating procedures, etc.) that guide the responses whose failures are represented by the HFEs have been tested and verified to be appropriate and that the response is feasible.
- Training is conducted on the procedures such that the methods of response are understood and have been practiced in the simulator or, for some of the more unexpected responses, using desk-top exercises.
- There is sufficient fidelity between the plant response to a given set of failures or an initiating event as modeled in the simulator and the expected plant response that there will not be any significant potential for developing an inappropriate understanding of the plant status and the required operator responses.
- The crew is experienced, well trained, and well-disciplined with good communication protocols. The crew complement (shift staffing) is in accordance with the licensing requirements outlined in 10CFR50.54.
- Instrumentation required to implement the operating procedures is generally available and reliable. When instrumentation is significantly impaired, this will be reflected in the value of the HEP through explicit evaluation. However, depending on the nature of the indications,

single instrument failures are often considered to be compensated for by redundant instruments.

1.4 HRA Process and Report Structure

Figure 1-1 illustrates the general HRA process. HRA is generally comprised of the following high level tasks:

- *Scenario analysis and HFE Identification*: This step requires a systematic review of the event scenario evolution and applicable procedures to identify the relevant required responses, a definition of the accident sequences to include the impact of failing to perform the responses represented as human failure events (HFEs) consistent with the logic structure of the model.
- *Qualitative & Quantitative Analysis*: Develop an HFE narrative (including the expected response path and timeline, an assessment of relevant crew failure modes (CFMs), and performance influencing factors (PIFs). Assess the HEPs in a well-defined and self-consistent manner that accounts for plant- and scenario-specific influences on human performance and ensures feasibility of the final action.
- *Model Integration*: Perform a reasonableness check of HEPs and capture potential dependencies between actions in the same sequence. Model system recovery actions only if the recovery has been demonstrated to be plausible and feasible for the scenarios applied and account for uncertainty and dependencies on earlier human failures in the scenario. (The impact of human performance can represent an important source of uncertainty in the numerical results of a PRA).

While the IDHEAS General Methodology covers the whole process shown in the diagram, the specific guidance in IDHEAS for internal at-power application begins at the qualitative analysis of identified HFEs in a given PRA scenario. Analysts can use the guidance in IDHEAS General Methodology when analyzing scenarios and identifying HFEs for internal at-power events. Thus, this report structure generally mirrors the lower portion of the diagram. The report is comprised of the following chapters:

- Chapter 2 provides an overview of the IDHEAS process. The overview includes a high-level description of the guidance for scenario analysis and HFE identification although the detailed guidance is not included in this report.
- Chapter 3 provides guidance for performing a feasibility analysis to ensure that the actions associated with the HFEs being modeled can be performed. The process and criteria for determining the feasibility of an action, including guidance for evaluating timing elements necessary for the analysis are described. The chapter also provides guidance on analyzing the effect of time uncertainties, and for addressing time-critical actions.
- Chapter 4 provides guidance on the performance of a detailed task analysis (both cognitive and execution) and the construction of crew response diagrams (CRDs) and associated time-lines, which are developed for this method to support a consistent and thorough assessment of the possible scenario progression (success and failure paths) in sufficient detail to support quantification.
- Chapter 5 provides a description of the quantification model. The quantification model is comprised of a set of decision trees (DTs) representing various crew failure modes (CFMs). The DTs capture the relevant performance influencing factors (PIFs) for each CFM. Specific guidance, in the form of questions, is provided to aid the analyst to consistently evaluate the branch points of the DTs.
- Chapter 6 provides guidance in implementation of the quantification model described in Chapter 5 to estimate an HEP through the interface provided by the CRDs developed in Chapter 4.

- Chapter 7 provides guidance on integrating the HRA with the PRA, including topics such as cut set review, recovery, dependency and uncertainty.
- Chapter 8 provides an overview of items needing further consideration and resolution before the final publication of this method.
- Appendix A provides an example demonstration of the IDHEAS method applied to three example HFEs.
- Appendix B provides a summary of the lessons learned from existing HRA methods and activities.
- Appendix C provides a mapping of the crew CFMs to the macrocognitive functions, proximate causes and cognitive mechanisms to show the applicability of relevant PIFs to the DTs.
- Appendix D gives an overview of the expert elicitation process and the results.

Overall HRA Process

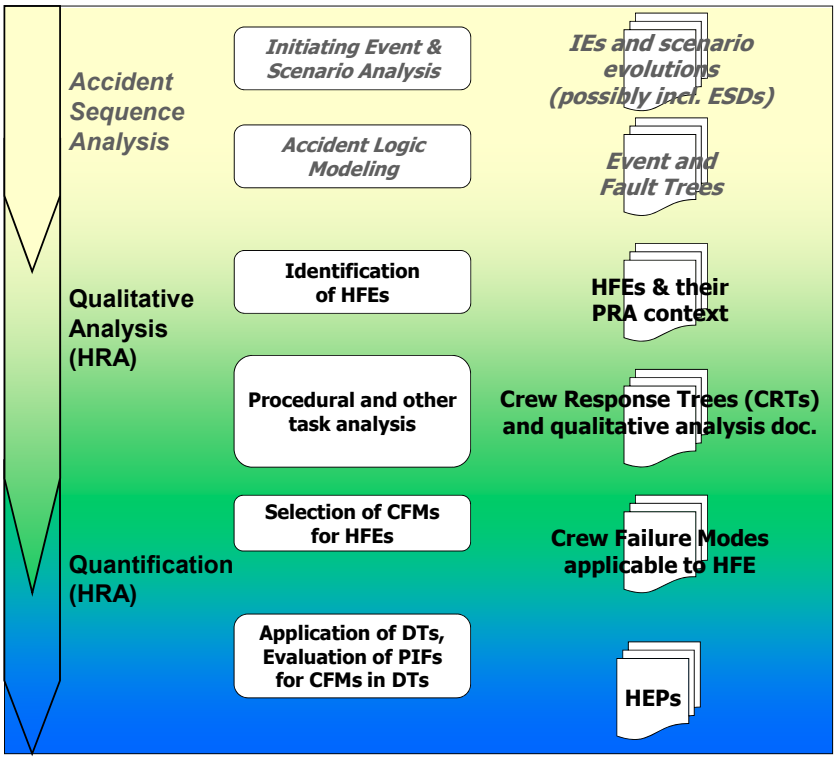


Figure 1-1. IDHEAS and how it fits in the overall HRA process

1.5 Continuous Development and Improvement of HRA

There are several regulatory applications in which HRA plays a significant role. Examples are: the significance determination process, risk-informed licensing changes, fire analysis, precursor analysis and detailed PRAs for existing as well as future reactors. In addition to these regulatory applications, industry is using PRA/HRA for decision-making. For these applications, adaptability/scalability is one of the desirable features of the method, and probably a very

important one. The existence of different HRA methods reflects the need to have tools available suitable to the specific application needs. For example, ASEP [14] was developed as a simple alternative to THERP [15], which is resource-intensive. Also, SPAR-H [16] was developed as a simple tool to screen human events to support NPP event analysis. Even if we try to focus specific methods to specific applications, analyst-to-analyst variability will be an issue in addition to a specific method's capability to correctly handle human performance in the specific application.

Finally, we would like to point out that, while we focused on the aims mentioned in the beginning of this chapter throughout the development process of IDHEAS, there are a number of issues that need to be addressed in order to make IDHEAS a practical tool as discussed in Chapter 8. Furthermore there is a need to test the method to demonstrate that the aims and the overall objective of reducing HRA variability are achieved, and finally guidance on how to use the method needs to be developed. Moreover, completing the initial development of the method was just the first step in our long term goal for improving HRA. The method itself may need improvement and enhancement as new lessons are learned in applications, new knowledge of human performance and human error become available, and new requirements for HRA are raised.

1.6 References

1. "Use of Probabilistic Risk Assessment Methods in Nuclear Activities: Final Policy Statement," Federal Register, Vol. 60, p. 42622 (60 FR 42622) (August 16, 1995).
2. US Nuclear Regulatory Commission. Staff Requirements – Meeting with Advisory Committee on Reactor Safeguards, SRM MO61020. US Nuclear Regulatory Commission, Washington, DC, 2006.
3. Letter dated Apri 23, 2007, from William J. Shack, Chairman, ACRS to Dale E. Klein, Chairman, NRC, Subject: Human Reliability Analysis Models, ACRSR-2247.
4. Lois, E., Dang, V. N., Forester, J., Broberg, H., Massaiu, S., Hildebrandt, M., Braarud, P. Ø., Parry, G., Julius, J., Boring, R., Männistö, I., & Bye, A. (2009). International HRA Empirical Study – Phase 1 Report: Description of Overall Approach and Pilot Phase Results from Comparing HRA Methods to Simulator Data. (NUREG/IA-0216, Vol. 1). Washington, DC: US Nuclear Regulatory Commission.
5. Bye, A., Lois, E., Dang, V. N., Parry, G., Forester, J., Massaiu, S., Boring, R., Braarud, P. Ø., Broberg, H., Julius, J., Männistö, I., & Nelson, P. (2011). International HRA Empirical Study – Phase 2 Report: Results from Comparing HRA Method Predictions to Simulator Data from SGTR Scenarios. (NUREG/IA-0216, Vol. 2). Washington, DC: US Nuclear Regulatory Commission.
6. Forester, J., Liao, H., Dang, V. N., Bye, A., Presley, M., Marble, J., Broberg, H., Hildebrandt, M., Lois, E., Hallbert, B., and Morgan, T. (2016). Assessment of HRA Method Predictions Against Operating Crew Performance on a US Nuclear Power Plant Simulator (NUREG-2156, Draft Report). Washington, DC: US Nuclear Regulatory Commission.
7. Memorandum of Understanding Between U.S. Nuclear Regulatory Commission and Electric Power Research Institute, Inc. on Cooperative Nuclear Safety Research, 2007 (ADAMS: ML070740114).
8. Memorandum of Understanding Between U.S. Nuclear Regulatory Commission and Electric Power Research Institute, Inc. on Cooperative Nuclear Safety Research Probabilistic Risk Assessment (PRA), 2010 (ADAMS: ML100490657).
9. Whaley, A. M., Xing, J.,Boring, R. L., Hendrickson, S. M. L., Joe, J. C., LeBlanc, K. L., & Lois, E. (in preparation). Building a Psychological Foundation for Human Reliability Analysis. (NUREG-2114, INL/EXT-11-23898). Washington, D.C.: U.S. Nuclear Regulatory Commission.

10. Hendrickson, S. M. L., Forester, J. A., Dang, V. N., Mosleh, A., Lois, E., & Xing, J. (2012). HRA Method Analysis Criteria. Proceedings of the 11th International Conference on Probabilistic Safety Assessment and Management (PSAM11), Helsinki, Finland.
11. 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.
12. Kolaczkowski, A., Forester, J., Gallucci, R., Bongarra, J., & Lois, E. (2007). Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire. (NUREG-1852). Washington, DC: US Nuclear Regulatory Commission.
13. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, The American Society of Mechanical Engineers, New York, NY, February 2009.
14. Swain, A. D. (1987). Accident Sequence Evaluation Program Human Reliability Analysis Procedure. (NUREG/CR-4772; SAND86-1996). Washington, DC: US Nuclear Regulatory Commission.
15. Swain, A. D. & Guttmann, H. E. (1983). Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications. (NUREG/CR-1278; SAND80-0200). Washington, DC: US Nuclear Regulatory Commission.
16. Gertman, D. I., Blackman, H. S., Byers, J., Haney, L., Smith, C., & Marble, J. (2005). The SPAR-H Method. (NUREG/CR-6883). Washington, DC: US Nuclear Regulatory Commission.

2 AN OVERVIEW OF IDHEAS

This chapter presents an overview of the IDHEAS HRA method and how its elements support the PRA process. IDHEAS was developed to support an HRA that is being performed to support a PRA model. A crucial task therefore is the identification and definition of the HFEs that are to be included in the logic model. However, development of guidance for this task was not a primary objective of the IDHEAS development described in this document, since this is addressed in other guidance documents, such as NUREG-1792 [1], ATHEANA [2], SHARP1 [3], and NUREG-1921 [4]. Nevertheless, since the development of the PRA model is an iterative process, there are aspects of the IDHEAS HRA model that can influence the definition of accident scenarios. For example, if specific sets of performance influencing factors (PIFs) can lead to high likelihood of failure, it may be advisable to modify the model to include accident scenarios that generate challenging PIFs.

It has to be remembered that a PRA model is a representation of the spectrum of potential accident scenarios. The accident scenarios constructed for a PRA are idealized, representative scenarios each of which typically represents the bounding case for the whole class of scenarios with similar characteristics. Where the scenarios that are encompassed by the representative accident scenario differ is in a level of detail that is not modeled. Examples of assumptions that are inherent in the definitions of the representative accident sequences include:

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

As will be discussed, the functional definition of the HFEs identifies those specific PIFs that are scenario specific, i.e., those that can be determined from the accident scenario definition and the plant status evolution that results. Thus the initial definition of HFEs is determined by the level of detail with which the scenarios are modeled. Determining the appropriate level of detail for the accident scenario descriptions can be challenging when using a PRA to evaluate the significance of an event (e.g., ASP) or a performance deficiency (SDP), since the boundary conditions may be different from those used in a PRA model used for prospective analysis.

Depending on the specific HRA method used, additional PIFs are taken into account when evaluating the HEP. These PIFs are used to assess the scenario-specific factors that influence the reliability of the operators' response.

An important assumption when using HRA models in a PRA is that, because the time at which an initiating event may occur is considered random, the HEPs are intended to represent an average over crews, time of day, and other plant conditions that could be coincidental with the failures defining the PRA scenario for which the HFE is being evaluated, but are not such that attention is essential but could potentially be distracting. When performing a PRA analysis for a scenario in which coincidental failures are to be modeled as boundary conditions (e.g., for an ASP analysis), their impact as distractors will be taken into account explicitly when assessing the PIFs.

2.1 The HRA Process and the Elements of IDHEAS

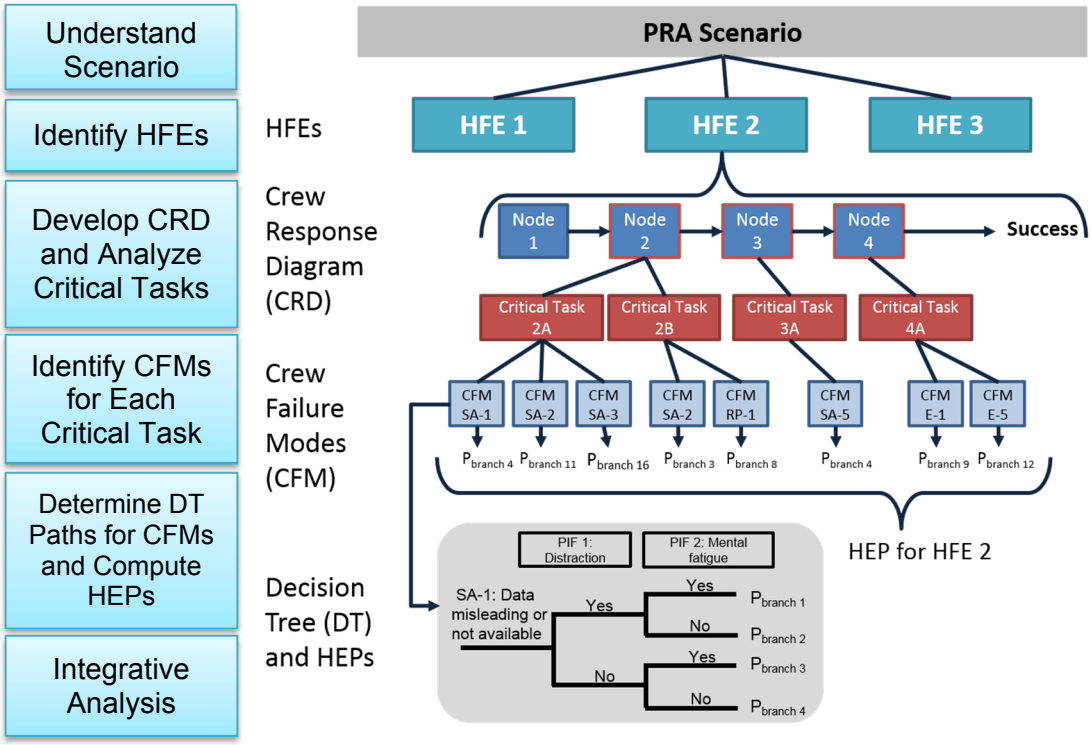


Figure 2-1 IDHEAS process

Figure 2-1 illustrates the IDHEAS process. The main steps of the HRA process and the way in which the elements of IDHEAS are used in each of these steps are listed in Table 2.1. The key IDHEAS elements include the performance of a task analysis, the development of Crew Response Diagram (CRD), and the implementation of the quantification model to estimate the HEPs. In addition, an essential element of the HRA process is the performance of a feasibility analysis. Since this can be done at any point during the HRA process, it is not highlighted as a separate step, but could be considered as a continuous activity. Guidance for performing a feasibility analysis is discussed in Chapter 3.

The CRD is a graphical representation of the results of a task analysis to identify the high level tasks that are necessary for successful response and which, if performed incorrectly, would lead to the HFE, and is the framework within which the quantitative analysis is performed. In addition, the CRD includes identification of opportunities for recovery given an initial failure. The paths through the CRD (including failure to recover) are called crew failure paths. The quantification model is developed as a set of Crew Failure Modes (CFMs) and associated Decision Trees (DTs). The CFMs represent different ways in which the crew may have been observed to fail. The DTs are structured to address the PIFs that can influence the occurrence of the CFMs.

Although the HRA process steps may be performed using other conventions and the quantification elements of IDHEAS, i.e. the CFMs and the DTs, may be applied without the CRD, one of the aims of IDHEAS is to provide guidance for a systematic, structured HRA process from identification, through qualitative analysis, to the quantification of the HFE.

Table 2-1. HRA process steps and IDHEAS elements

HRA process step	Products of the step	IDHEAS elements (and report section)
Accident scenario analysis and operational story	Description of accident scenario, operational story characterizing main human performance challenges in the scenario	Not included in this report. See IDHEAS General Methodology
Identification and definition of HFEs	Set of HFEs and their definitions	This report assumes that the set of HFEs has been identified and defined functionally as part of the development of the PRA model. See IDHEAS General Methodology for guidance on HFE identification.
HFE feasibility analysis and time uncertainty analysis	HFE feasibility and effect of time uncertainties	HFE feasibility, time uncertainties and their contributions to HEP, in Chapter 3
Procedural task analysis	Identification of critical tasks required for successful response and the requirements, inputs, and guidance for tasks and tasks; identification of crew failure paths (HFE failure scenarios); error recovery (correction) potential and development of CRD; development of time line.	Crew response diagrams (CRDs), notation, the qualitative analysis process, and example analysis, in Chapter 4
Implementation of the quantification model - identification of applicable CFMs and application of the DTs	For each HFE, identification of the CFMs applicable to each crew failure path, quantification of each CFM though the use of the DTs, HEP for the HFEs (before consideration of dependencies)	Quantification Model - Identification of CFMs and crew failure scenarios (DT paths) in Chapter 5, and use of DTs in Chapter 6
Integration – results review, documentation, dependency analysis, and recovery actions	HEPs after review and consideration of dependencies. Identification and analysis of recovery actions, Analysis of uncertainties, Final documentation.	Model Integration, Chapter 7

While the steps of the HRA process are shown here sequentially, in practice, almost all of these steps are iterative. As the HRA evolves through these steps, it also evolves with the PRA the HRA supports. As such, the inputs to the HRA potentially come from several PRA tasks. For example, timing information necessary for HFE quantification and cable tracing for instrument reliability may come largely from the PRA. Furthermore, the potential for adverse environments and timing information relative to equipment damage comes from the understanding of the PRA scenarios for which the HFEs are defined.

Each of the steps of the overall HRA process shown in Table 2.1 are described at a high level in the following sections.

2.2 Scenario analysis

The objective of accident scenario analysis is to develop operational narratives that adequately describe the entire context of the evolving event scenario, how that scenario affects information and stimuli in the operators' environment, and factors that may influence personnel response in that context, considering the effects on all plant systems and functions. Scenario analysis analyzes a PRA scenario with a focus of understanding operator actions and challenges. The analysis allows for HRA analysts to gain perspective for the complete spectrum of scenario-specific conditions that may require operator attention. That perspective is essential for an analyst to perform an integrated assessment of all factors that may influence personnel performance in the context of the evolving scenario. The output of a scenario analysis is referred to as operational narrative.

2.2.1 Document initial condition, initiating event, and boundary condition

The initial condition is the status of the plant and crew before the initiating event.

- Plant operation status

- Significant plant configuration and unavailable components
- Staffing and ongoing activities

An initiating event is an event originating from an internal or external hazard that caused a plant abnormality requiring successful system automatic interventions, human interventions, or both to protect plant safety.

The boundary condition is the plant, site and crew status immediately after the initiating event. The boundary condition specifies the effects of the initiating event on the plant structure, systems, and components (SSCs) and instrumentation including:

- The plant automatic responses
- The initiating event's effects on SSC availability
- The effects of the SSC abnormality or damage on the plant staff responding to the event.
- The end consequence - the end point for the PRA/HRA analysts to determine scenario termination.

2.2.2 Develop the baseline scenario

The baseline scenarios should include a description of the scenario with the appropriate level of information detail to understand the scenario progression and the inclusion of the operation experience related to the scenario for the analysis. A timeline may need to be constructed to provide an understanding of the baseline scenario, including a description of the initial plant and staffing condition and other background information to this scenario (e.g., type of reactor, unique plant system, unique plant configuration, and latent component failures) at the beginning of the timeline.

The baseline scenarios can be divided into two classes:

- For PRA analysis: The analyses analyze hypothetical events. The baseline scenario is the expected scenario progression path from the operator trainers' perspective based on the given initial condition, initiating event, and boundary condition. The baseline scenario provides an understanding of the expected operator responses to the event according to their training and procedures.
- For the event analysis of the SDP and ASP processes: The analyses analyze the boundary conditions created by actual events. However, the conditional core damage frequency or probability is based on the PRA model with these boundary conditions imposed. This will influence the assessment of the PIFs necessary to analyze the HEPs.

2.2.3 Perform context analysis

The purpose of context analysis is to identify the context (situations and conditions) that challenges plant and human performance in the scenario. The documentation of the context serves as the high-level guidance for HFE definition and analysis, although not every item in the context applies to all the HFEs. Context analysis is to provide a basis to estimate the HEPs of the interested HFEs. The context is divided into the following three sub-context groups:

- The plant context - The plant context provides a bird's-eye view of the scenario for a holistic understanding of the scenario progression before diving into the details analysis of specific HFEs.
- The crew context - Crew context is centered on the conditions that affect the crew performance of key actions. This includes the information, stimuli, and conditions, etc. affecting the crew's ability to perceive the information related to the plant abnormality, understanding the situation, making correct decisions, and performing the required actions in time to prevent an undesired consequence from happening. All of the above mentioned

human activities are most likely to be performed in a teamwork environment. Identification of operational challenges should be based on the understanding of how these macrocognitive functions are performed.

- The task (to be performed) context - Task context refers to the factors that challenge personnel tasks in HFEs.

2.3 Identification and Definition of HFEs

2.3.1 Identification of HFEs

A human failure event (HFE) is defined as part of a PRA scenario. It is defined as a failure to perform a required function in response to the particular plant status, e.g., an unavailability of a system or function, or the initiation of a function following an initiating event. The failure is the result of one or more errors.

Several sources provided guidance on identifying and defining HFEs such as the NUREG-1792 [1], ATHEANA [2], SHARP1 [3], and NUREG-1921 [4]. Each of these methods was reviewed to provide the guidance presented here. Currently, the Fire HRA Guidelines presented in NUREG-1921 [4] represents the state-of-practice and is the primary guidance adapted here for IDHEAS.

Identifying the HFEs to be modeled in PRA requires working with PRA analysts to develop a base event sequence in the PRA model with input from the baseline scenario developed in the previous step. Additional HFEs are identified by identifying and developing other event sequences for the scenario by asking "What-If" questions.

When identifying the initial selection of HFEs to quantify, the HRA analyst should work with the PRA team. Guidance is provided in multiple sources on the composition of a multi-disciplinary HRA team to ensure a thorough review and inclusion of relevant human-system interactions [1 - 3]. The HRA analyst should be called upon during the development of the initial plant PRA model to ensure completeness of the model.

This report is primarily focused on post-initiator HFEs. That is, those human actions that take place after an initiating event has occurred. These represent actions taken either while following procedures or performing recovery actions in response to the initiating event. Pre-initiator[1] and initiating event[2] HFEs may also be considered, but are not covered here, except as indicated below. For further guidance on the identification of pre-initiator human events, the Good Practices [1] provides a summary of steps that should be completed for a thorough review.

HFEs due to a response failure[3], i.e., those events that represent the impact of human failures committed during actions performed in response to a plant disturbance (e.g., while following post-trip procedures (post-initiating events) or performing other recovery actions that could preclude an initiating event such as starting the redundant CCW train given failure of the operating train) should be included in the model as they may have a direct influence on the mitigation or exacerbation of undesired plant conditions after the initial plant upset. Identification

---

[1] Pre-initiator human interactions take place before the initiation of an accident sequence and represent human failures in inadvertently disabling, mis-positioning, or failing to restore equipment following calibration, test, or maintenance activities. These actions make the equipment unavailable when needed during the accident scenario.

2 Initiating event human interactions are those human events that contribute to the occurrence of the initiating event. The effects of initiating event human interactions are often accounted for in the initiating event frequencies obtained from plant operating experience [3]. However, if the initiating events are analyzed using system models, those models may include HFEs that have the characteristics of either pre-initiator HFEs or have the characteristics of a post-initiator HFE in that they represent failure to respond to an annunciated failure.

3 These HFEs primarily involve post-initiator human actions but may also include those HFEs that are included in system models for initiating events.

of these HFEs to be included in the PRA model focuses on the operator actions that will be taken in response to a variety of possible accident sequences. These actions result in failures that, in combination with equipment failures, may result in core damage or lead to a large early release.

The primary source of information in determining HFEs involving response failure will be a review of all relevant procedures and guidelines including:

- System or normal operating procedures
- Emergency operating procedures (EOPs)
- Abnormal operating procedures (AOPs)
- Annunciator procedures
- System operating procedures
- Severe accident management guidelines (SAMGs)
- Other special procedures as appropriate (e.g., fire emergency procedures)

An additional source of information comes from actual experiences in responding to operational disruptions, plant trips, etc. Walkdowns and talk-throughs with plant operators or observations of simulator exercise may also provide useful information and help analysts with understanding the procedures and how they are implemented by the crews. For identification of HFEs involving special circumstances (e.g., fire or seismic HFEs), the analyst should make use of special procedures and the experience of operations and training personnel to aid in understanding how the procedures are interpreted and implemented as operator actions and, therefore, as potential HFEs.

The goal in the reviews of procedures, historical data, and interviews is to identify ways in which crews are intended to interact with the plant equipment after an initiator. The ways they interact will be a function of the various conditions that can occur, as defined by the development of the PRA accident sequences and associated equipment unavailability and failure modes. To meet this goal, analysts should particularly note where operator actions that will directly influence the behavior of the system or affect critical functions are called out in these procedures and under what plant conditions and indications (cues) such actions are carried out. (Note: some actions may be performed immediately and without regard to the specific situation, while others will be plant status and cue dependent.) 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.

During the review of post-initiator related procedures, the functions, associated systems and equipment modeled in the PRA should be identified. It is necessary to understand whether the function is needed or undesired for each scenario addressed. Then, the system and equipment should be identified regarding their impact on the function – that is, how they contribute to performing the function or have caused the undesired condition. In the identification process, ways in which the equipment may functionally succeed or fail should be understood and included.

Once the functions, systems and equipment have been identified and understood, the analysts may work on identifying the human actions important in the interactions with aforementioned elements. That is, the ways in which the operators intend to or are required to interact with the equipment credited to perform the functions modeled for the accident sequences included in the PRA, as well as how the operators will respond to equipment and failure modes that may cause undesired conditions per the PRA, need to be identified. If a scenario is identified for which the procedures do not apply, or the response cannot be shown to be feasible, no credit is taken for

the operator response; if an HFE is included in the model as a placeholder for example, its probability should be set to 1. Further, if the required instrumentation is unavailable, the HFE would again be set to 1, unless an argument could be made that alternative cues were available.

While identifying the post-initiator human actions, certain types of actions are not expected to be included such as those performed without any procedure guidance or those not trained on. Instead, the action included or credited with the analysis will most likely resemble the following:

- Actions that are necessary and desired or expected given the scenario
- Back-up actions to failed or otherwise defeated automatic responses (NUREG-1792 [1] cautions to be sure that the action can be credited to recover the auto-failure mode)
- Anticipated procedure-guided or skill-of-the-craft recovery actions
- Actions that require permission from other emergency or technical support staff

Although many of these actions will be included as errors of omission (EOOs), errors of commission (EOCs) should be considered where applicable as well. EOOs represent failures to take the appropriate actions as called out in the procedures or as trained on or as expected given the scenario. NUREG-1792 [1] points out that possible actions for which failure would involve an EOC have generally been beyond PRA practice, but some issues may require that the PRA/HRA address such failures.

2.3.2 HFE Definition

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 [5] outlines the requirements for definition. 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 [2, 3, 4]:

- Accident sequences, the initiating event, and system and operator action successes and failure subsequent to the initiating event and preceding the HFE
- Accident sequence-specific procedural guidance
- 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
- The cues and other indications for detection and evaluation of errors

Once this information is gathered, the HFE can be defined at the level describing the human failure of not properly performing the action and linking it to the affected component, train, system, or function. The definition should include what the consequences of the failure are and where those consequences are likely to be located (i.e., at the component, train, system, multi-system, or function level).

Much of the detailed definition of the HFE will be completed with the qualitative analysis. In fact, the identification and definition of the HFEs may be seen as an iterative process expanded upon with the qualitative analysis.

2.3.3 Initial Assessment of Feasibility

Once the operator action has been identified and the HFE defined, the HRA analyst needs to do an initial assessment of whether the operator action is feasible. The purpose of the initial feasibility check is to eliminate from the PRA model any operator action that is clearly not possible given the scenario. At this stage in the HFE development, the feasibility assessment is primarily conducted using information obtained during the HFE definition supplemented by any additional information that may be known about the particular action or PRA scenario. This initial assessment should be based on the criteria described below, but note that any EOP based actions can initially be considered feasible and should be carried forward in the analysis. However, feasibility should be treated like a "continuous action step" and reviewed periodically as the HFE is further developed and refined. Chapters 3 and 4 provide information on how to perform a more detailed assessment of feasibility as more information is obtained.

The questions presented immediately below can be used to perform the initial feasibility assessment of HFEs given the information that may be available at this stage of the analysis. If the questions can be answered with the available information and it is clear that the HFE would not be feasible, the HFE should not be included in the model or the HEP should be set to 1.0. Otherwise, the HFE should be included in the model and re-evaluated later when more detailed information is obtained during stages described in Chapters 3 and 4):

- **Is there sufficient time to complete the action?** While a detailed timing analysis is not required at this point, using the available timing information from the identification and definition of the HFE, the analyst should assess whether there is sufficient time available to complete the action. If it is obvious that there will not be enough time available, the HFE should not be included in the model or the HEP should be set to 1.0. This item involves examining both the total time required to accomplish the action and the time available. The total time required for the action consists of the amount of time required for diagnosis and the amount of time required for execution (including transit time). The total time required must not exceed the total time available to complete the action. The total time available can be estimated based on thermal-hydraulic calculations, simulation data, or engineering judgment as is traditionally done in PRA.[4]
- **Are there sufficient cues available for diagnosis?** The analyst should ensure that there are sufficient cues for diagnosis. If all of the cues for diagnosis are impacted by the initiating event such that the action cannot be performed, the action is considered not feasible.
- **Is the location where the action is to be accomplished accessible?** If actions are to be performed locally, the location of the action as well as the route must be accessible. If the area or route is not accessible, the HFE should not be included in the model or the HEP should be set to 1.0.
- **Is there enough staff available to complete the action?** If there are not enough crew members available to complete the action (the number of people required for each task exceeds the crew available), then the HFE should not be included in the model or the HEP should be set to 1.0.
- **Is all the equipment needed to perform the required critical tasks available?** This item includes instrumentation and/or alarms and component operability considerations. There must be at least one channel of instrumentation and/or alarms for cue(s) for an operator action to be feasible. Similarly, the components manipulated during the operator response must be free of damage. If the initiating event has damaged the equipment such that it will

[4] Although such a detailed judgment is not necessary for this initial feasibility assessment, Chapter 3 presents detailed guidance on estimating the amount of time required.

not function (even if the operator takes the appropriate action), then HFE should not be included in the model or the HEP should be set to 1.0.

In the identification and definition stage, the HFE narrative and information about each performance influencing factor (PIF) is likely not yet known. Thus, this initial evaluation should be based on the available information with the knowledge that as the additional information becomes available, the feasibility step should be reassessed as described in Chapters 3 and 4 for those HFEs that have not been eliminated.

2.3.4 Time uncertainty analysis

The purpose of this step is to identify uncertainties in the time available and time needed to perform the human actions in an HFE and to quantify the contribution of time uncertainties to the overall HEP of the HFE. The process is as follows:

1. Identification of factors contributing to time uncertainty that include:
   - Estimating distribution of time available for completing the task (time available)
   - Estimating distribution of time needed to complete the task (time demand)
2. Calculation of the contribution of time uncertainties to the HEP

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 is all types of operator failures other than Pt. Pc will be calculated from the IDHEAS quantification model.

Pt – Error probability introduced by the time factor in the HFE. This assumes that the crew follows their protocol or procedures correctly and there are no additional complications (e.g., equipment failures) except as specified in the initial condition, initiating event, and the boundary condition. **Pt** is caused by the likelihood that the time available to perform the human action is less than the time needed for the action. Psychological time pressure (even if there is enough time) also impairs task performance and may lead to errors, but it is treated as a PIF, so it does not contribute to **Pt**.

Pt is calculated with the time-reliability model as follows:

1. Estimate probabilistic distributions ((the central tendency and range, e.g., 5^{th}, 50^{th}, and 95^{th} percentile) of the time available (T_{avail}) and time needed (T_{needed}) to perform the HFE. Guidance is provided for estimating the distributions.

   Estimating T_{needed} should consider three key aspects: time contributors, modification factors, and bias factors (i.e., the information that may be missed due to the biases):

   - Acquire the Initial estimation of T_{needed} from PRA models or plant information.
   - Verify T_{needed} by checking if the contributing factors are considered.
   - Adjust the time by estimating and accounting for the effects of the modification factors.
   - Adjust the time by considering the bias factors.
2. Calculate the convolution (Pt) of the distribution functions of T_{avail} and T_{needed}.

2.4 Task Analysis and the Development of Crew Response Diagrams (CRDs)

In an application of IDHEAS, the CRD is used as a graphical representation for the procedural task analysis. The development of the CRD for the HFE and the documentation of its nodes is a critical part of the qualitative analysis. This analysis begins with the initial cues for the required operator response in the PRA scenario context defined for the HFE in terms of the hardware

and operator action events (success or failure events) subsequent to the initiating event and leading up to the demand for the operator action. The qualitative analysis determines:

- Which procedures are applicable and in play in this scenario context
- The expected success path and critical tasks of the crew response, which consist of the decisions (including procedure transfers) that must be reached and the execution tasks that must be performed to achieve the functional goal
- The critical activities, addressing what must be done and the success requirements for each activity in order to complete the critical tasks
- The timeline of cues and the estimated time to reach specific points in the procedure (in the response) for the modeled PRA scenario

In this way, the qualitative analysis identifies the potential failures and the conditions that may contribute to these failures. Furthermore, it identifies the opportunities for error correction and the cues and procedural guidance that support these. Given the information on the timing of the cues and of the crew's response, the time feasibility of the HFE (and the feasibility aspects related to the cues) should be revisited at this stage.

Chapter 4 describes the procedural task analysis in detail and illustrates the development of the crew response tree and the accompanying documentation as the qualitative analysis proceeds through its stages (success path – cues and their timing – procedures – training; critical tasks; error correction potential).

2.5 Implementation of the Quantification Model

The CRD represents the expected success path, one or more crew failure paths corresponding to failures of the tasks on the success path, and the error correction opportunities (if any) identified for these failure paths. The nodes on the success branch on the CRD represent critical tasks or activities that if failed would lead to the HFE. IDHEAS quantification consists of implementing the quantification model described in Chapter 5 to the CRD using the following steps:

1. Identification of the CFMs applicable for the crew failure paths of the HFE.

The CFMs correspond to three high-level task types: status assessment (SA), response planning (RP), and action (A). The expected success path is the sequence of critical tasks, which if performed successfully and within the available time, will lead to the success of the operator action. Each of the crew failure paths (or HFE failure scenarios) corresponds to the failure of a critical task. Consequently, the CFMs applicable to the crew failure paths are identified by examining the tasks and their requirements, as discussed in section 6.2.2.

Multiple CFMs may be identified for a given crew failure path; in other words, the crew failure path may result from CFM1 *or* CFM2 *or* … etc. They would be alternative failure modes for the critical task, corresponding to the failure of different tasks (or, in some cases, to alternative failure modes for the tasks).

2. Identification of the appropriate path through the DT associated with each CFM.

The decision tree for each applicable CFM for a crew failure path is applied, answering the DT questions for the critical task as discussed in Section 6.2.3.

3. Calculation of the HEP for the HFE.

The combined HEP is the sum of crew failure path probabilities, where each failure path probability is the sum of the CFM probabilities (each determined by use of the DT and answering the questions associated with the DT branches based on the information collected in the qualitative analysis) as discussed in section 6.2.4.

At this stage, the combined HEP does not account for dependencies among HFEs.

2.6 Integration – Results Review, Documentation, Dependency Analysis and Recovery Actions

In this step, the HRA results are integrated into the PRA model. The main parts of this step are:

- Review of the overall PRA results (the accident sequences with the operator actions) for reasonableness, focusing on the HFEs shown to be important after integrating the HEPs in the PRA model
- Documentation of the HFE analysis to support the HEP
- Consideration of the dependencies among HFEs
- Analysis (identification) of recovery actions, beyond the error correction opportunities included in the CRT for the HFE.

Section 7.1 discusses the results review and reasonableness check. The analysis of dependencies among HFEs and the quantitative impact of dependencies are presented in Section 7.3. The identification of recovery actions is briefly discussed in Section 7.2.

2.7 References

1. 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.
2. Nuclear Regulatory Commission (NRC) (2000). Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). (NUREG-1624, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission.
3. Wakefield, D., Parry, G., Hannaman, G., & Spurgin, A. (1992). SHARP1: A Revised Systematic Human Action Reliability Procedure. (EPRI TR-101711, Tier2). Palo Alto, CA: Electric Power Research Institute.
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. ASME/ANS RA-Sa-2009, Addenda to ASME/ANS RA-S-2008, Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications, The American Society of Mechanical Engineers, New York, NY, February 2009.

3 HFE FEASIBILITY ASSESSMENT AND TIME UNCERTAINTY ANALYSIS

The feasibility analysis in HRA assesses whether the operator actions can be accomplished to ensure that the PRA is not crediting an operator action that is not possible [1-3]. Thus, the feasibility assessment is the qualitative consideration of whether the operator action is go/no-go in terms of whether it should be included in the model and quantified, considering the major performance influencing factors discussed below. If the action is not feasible, an HEP of 1.0 is assigned, or the HFE is not included in the PRA.

An initial assessment of feasibility can begin 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 response are not available. The assessment performed during this early phase of the analysis is essentially a reasonableness check to avoid including any action that is obviously not feasible and it does not require a detailed timing analysis. However, a more detailed assessment will be needed as the necessary contextual and timing information are obtained (e.g., during the development of the timelines for the crew response diagrams (CRDs) described in Chapter 4).

NUREG-1852 [7] provides guidance for conducting a thorough feasibility assessment in the context of fire operator manual actions. It identified a set of criteria with which the feasibility of human actions could be granted. The ASME/ANS PRA Standard [5] also incorporated criteria that should be evaluated for post-initiator events from the standpoint of feasibility. Moreover, NUREG-1921 [4] adapted the various criteria to the fire HRA domain in the context of developing guidelines for performing fire HRA and provided further guidance on determining whether the criteria are met. Given that NUREG-1921 captures the state-of-practice in feasibility assessment for HRA (even though developed for fire HRA), we adopted the NUREG-1921 feasibility analysis with additional development on time estimation and how to address the impact of time availability before quantifying HFEs.

An important part of demonstrating feasibility is assessing whether there is adequate time to perform the response. Section 3.3 provides guidance for assessing time feasibility. For actions determined to be feasible, a reliability assessment is performed to determine the HEP contributed from uncertainties in time and crew failure modes. The decision tree method described in Chapter 5 calculates the HEP of the crew failure mode, and the approach described in Sections 3.2 and 3.4 is to estimate HEP contributed from time uncertainties when the margin between the time available and the time required is small.

3.1 Feasibility Assessment Criteria

This section presents the feasibility assessment criteria. Failure to meet any one of these criteria leads the HEP to be set to 1.0 and the operator response should not be credited in the PRA. Therefore, the task analysis should clearly define the absolute, necessary conditions to perform the critical tasks with respect to these criteria. As implied above, note that some criteria, especially the sufficient time and cues for critical tasks, may not be appropriately assessed until the development of crew response diagrams (CRDs) and the associated time-line are performed as described in Chapter 4. As with many aspects of performing a PRA, establishing feasibility for the actions associated with various HFEs may be an iterative process that requires modifications to the analysis as more is learned about 1) the conditions under which the crews are interacting with the system, 2) opportunities for human errors and recovery, and 3) the timing of events and actions as the accident scenario develops.

3.1.1 Sufficient Time to Complete the Tasks

A key parameter for evaluating feasibility is *time*. HRA must evaluate whether the critical tasks for an HFE can be diagnosed and completed within the available time. Both the total time required to accomplish the action and the time available need to be determined. The total time required for the action consists of the amount of time required for diagnosis once the relevant cues have occurred and the amount of time required for execution (including transit time). The time required must not exceed the total time available to complete the action as determined by the time window for the response. If it does, the HEP should be set to 1.0, or the corresponding HFE is not included in the logic structure. The total time available can be estimated based on thermal-hydraulic calculations, simulation data, or engineering judgment as is traditionally done in PRA. Section 3.2 presents detailed guidance on estimating the amount of time required.

Timing for recovery paths should also be addressed. When crediting recovery of an HFE (i.e., recovery of crew failure to take appropriate actions or recovery of inappropriate actions) based on subsequent cues or events in the scenario, the time available for accomplishing the recovery actions must take into account the time elapsing before the cues for those actions would become available (this issue is discussed further in Chapters 4 - 6).

Similarly, for cut set recovery actions, the time to accomplish the task must be adequate considering the total time available for the new recovery action after the initial system alignment was found to be ineffective in preventing challenges that could lead to core damage.

3.1.2 Sufficient Manpower

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 the action (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.
- 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 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 personnel will have to be summoned from outside the MCR or from off-site, an assessment of how long it will take them to get to the control room 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.

3.1.3 Cues Available

This factor addresses the instrumentation and/or alarms used as the cue(s) for the operator response to answer the following question: Has the cue(s) been impacted such that diagnosis is not possible? In general, HRA assumes that all operator actions are taken in response to a cue or cues. If there are none, the operators will not respond. Cues can be instrumentation (indications), a procedure step, or a plant condition (symptom). Typically, there are redundant cues in the MCR. Operators are often able to diagnose the problems with secondary cues when

the primary cues (such as alarms) are not available. Thus, the assessment of cues for feasibility should include both primary and secondary cues.

3.1.4 Procedures and Training

The feasibility analysis should include evaluation of the availability of procedures that are needed for diagnosing and executing the necessary actions as well as operator's training on the use of the procedures. The procedures should:

- Assist the operators in correctly diagnosing the event (or needed actions) and the plant response
- Identify the appropriate preventive and mitigative actions, including the tools or equipment that should be used and where the action should be taken
- If the scenarios are considered to be challenging or unusual, reduce potential confusion from aspects such as event-induced conflicting signals, masking effects, or spurious indications or actuations

Training quality should be evaluated based on its ability to do the following:

- Engender operator familiarity with potential adverse conditions arising from an event as well as the actions and equipment needed to mitigate the event
- Allow operators to be prepared to handle departures from the expected sequence of events
- Provide the opportunity to practice operator response and bolster confidence that these duties can be performed in an actual event

Certain operator actions may be identified as *skill-of-the-craft* and credited on that basis although not specifically proceduralized. However, the feasibility of these actions would have to be justified through the performance of walk-throughs or talk-throughs or by an evaluation of existing job performance measures (JPMs) for the actions related to the particular HFE. This is consistent with ASME/ANS PRA Standard [5] Supporting Requirement HR-H2, which states that 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."

3.1.5 Accessible Location

For actions outside the MCR, if it is known that the operators will not be able to reach the location(s) of the required critical tasks in an event, the operator action should not be considered feasible, and the initial HEP should be set to 1.0.

The evaluation of "accessibility" mandates an evaluation of the travel path required for local actions and how such accessibility might be compromised by the initiating 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 walkdowns. Travel paths 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 timing of the HFE execution task(s) must 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.

All of these effects should be considered possible when determining the feasibility of performing an operator action in a given situation (e.g., within a fire situation).

3.1.6 Availability of Equipment Required for Critical Tasks

To access and manipulate plant equipment during local actions, portable and special equipment may be needed and should also be considered from the standpoint of feasibility. Items falling under this category according to NUREG-1852 [7] include keys to open locked areas (especially in light of tighter key controls that some plants may have implemented in response to security needs) or keys that allow manipulation of locked controls, portable radios, portable generators, torque devices to turn handwheels, 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.

3.1.7 Operable Relevant Components

This criterion addresses the need to ensure that the equipment that is necessary to enable implementation of an operator action to respond to an event is available and not damaged or otherwise adversely affected by the event (PRA scenario).

Implicit in this feasibility criterion is the presence of a human-system interface (HSI) that was assumed to be adequate for the actions and an assumption that the operators have the ability to properly evaluate and address the event conditions in order to maintain plant functionality.

If the equipment is damaged such that it will not function even if the operator takes the appropriate action, the operator action should not be considered feasible, and the HEP should be set to 1.0.

3.2 Guidance on Time Estimation Addressing Uncertainty

NUREG-1852 [7] and NUREG-1921 [4] present a structured timeline to estimate time for an individual HFE (see Figure 3-1). 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.

3.2.1 Definitions

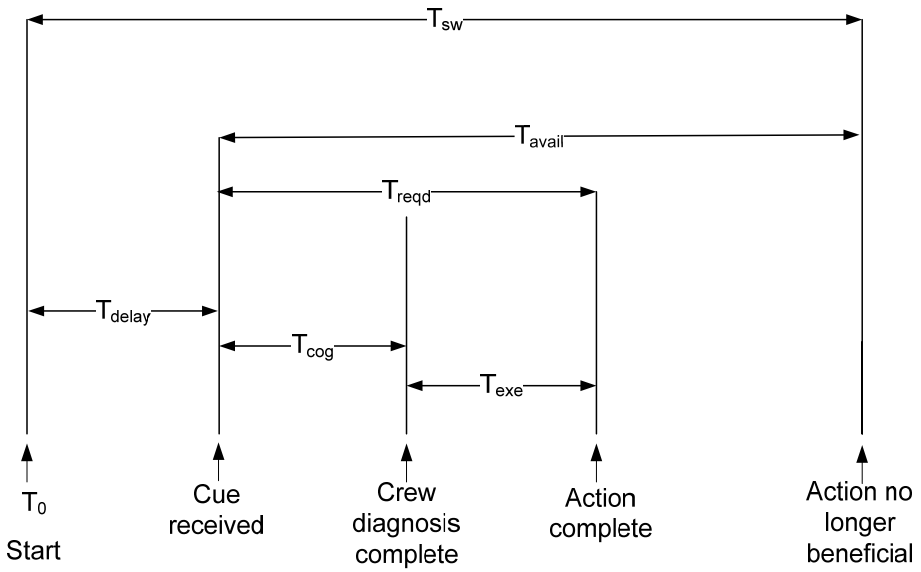


Figure 3-1 Timeline illustration diagram

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 3-1, 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 for the representative PRA scenario and, for HRA quantification, is considered to be a fixed 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.

3.2.2 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:

1. Obtain an initial distribution of time including the central tendency and range (e.g., the 10^{th}, 25^{th}, 50^{th}, 75^{th}, and 90^{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.
2. 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 $T_{exe.}$
3. 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 $T_{exe.}$
4. 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 to 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 (rain, wind, coldness, heat, darkness, etc) Flood Fire (and smoke, heat) Seismic Others
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-making infrustructure	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	Variabilities in crew experience and training Individual variability
Others	

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.

3.2.3 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 as 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, f_T.

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 1.5 h. 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.

3.3 Consideration of Timing Results Before Use of the IDHEAS DTs

The purpose of the analysis of feasibility is to assess the qualitative consideration of whether an operator action associated with an HFE is go/no-go in terms of whether it should be included in the model, considering the major performance influencing factors as discussed in Section 3.1 above. If the action is not feasible, an HEP of 1.0 is assigned, or the HFE is not included in the PRA (i.e., no credit is taken for the response). For actions determined to be feasible, a reliability assessment (i.e., the quantitative evaluation of the likelihood of success of the operator action; the derivation of the HEP for the HFE) is performed. In the IDHEAS method, a set of decision trees (DTs) are used to determine the HEPs for each of the relevant crew failure modes (CFMs) for a given HFE, which are combined to obtain the overall HEP for the HFE. An underlying assumption of the DTs is that the actions are feasible from a timing perspective. That is, it is assumed that there is adequate time available for the operating crew to diagnose the need for and complete the actions for a particular HFE.

However, as recognized in Section 3.2, 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. The guidance in section 3.2 directs analysts to obtain an estimate of the distributions of system time available for crew response and time needed for crew response time. The distribution of time needed gives an estimate of the time by which the slowest operating crews would be expected to complete the cognition and execution portions of the response. In other words, the maximum time it would be expected for all of the crews to complete the actions required, under the conditions presented in the scenario. While the guidance provides considerable information on how to consider a range of PIFs that could impact the time required and produce as realistic estimate as possible, 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. In such cases, it would not be appropriate to quantify the human actions with the IDEAHS DTs and therefore it is important to demonstrate that there will be adequate time to allow quantification of the actions. To address this issue in using the IDHEAS quantification model, two options are offered. Either option can be used to determine whether it is appropriate to continue with use of the DTs for quantifying an HFE. When the response is considered time critical, the IDHEAS quantification model is not adequate. HEP quantification for time critical actions should include the contribution from the CFMs and the time uncertainty, i.e., the likelihood that the time available for an action is less

than the time needed. One approach is to use a time reliability curve, such as the HCR/ORE [6]. An alternative approach is presented in Section 3.4.

3.3.1 Maximum Time Requirement

In the first approach, if the estimate of the maximum time required for the actions of an HFE has been conscientiously performed and analysts have confidence that the maximum time required would only be exceeded under rare circumstances, then as long as the maximum time required is less than the time available, then the actions can be quantified using the IDEAHS DTs. If there is uncertainty on the part of the analysts regarding the maximum time required, then it may be reasonable to ensure that there would be some time margin available (how to calculate time margin is described below) to account for the uncertainty in the estimates. If analysts are not confident that there is an adequate time margin, then either the HEP will have to be assumed to be 1.0, or the analysts will have to perform and document a more thorough analysis of the time required. Keep in mind, however, that procedure based actions (e.g., those in EOPs, alarm and abnormal plant procedures) have been vetted in terms of whether there should generally be enough time available for the actions, so a reasonable analysis that demonstrates that the available time should be more than the maximum time, should be acceptable to allow use of the DTs. Yet, if unusual or challenging conditions are expected (e.g., where instruments have failed or conditions could be masking the true plant status) or they could be present in the scenario with a relatively high frequency, then a higher time margin might be needed to account for uncertainty in the estimates in such situations.

3.3.2 Time Margin

In the second approach, analysts should first calculate the time margin for a particular HFE using the timing terms previously defined in section 3.2, but in this case the estimate of the average crew response time should be used rather than the maximum time. *Time margin* is defined as the ratio of time available for the action to the time needed to perform the action; it is calculated using either of the following equations:

$$Time\ Margin\ (TM) = \frac{T_{avail} - T_{needed}}{T_{reqd}} * 100\% \qquad \text{(Equation 1)}$$

In this approach, if the obtained time margin is a factor of two or more greater than the estimated time required (100% time margin), then it can be assumed that at least for procedure based actions, that there will be adequate time for the action and the HEP for the HFE obtained using the IDHEAS DTs can be used. However, if the time margin is less than 100%, then either the HEP will have to be assumed to be 1.0, or the analysts will have to perform and document a more careful analysis of the time required and/or a thorough justification to show that a smaller time margin would be adequate to ensure feasibility for the action and that the HEP obtained from the DTs are appropriate to use. In performing this analysis, analysts should show that given aspects such as the nature of the actions (e.g., short versus long timeframe events, simple versus complex actions, etc.) and/or consideration of the estimated maximum time, a smaller time margin would be adequate to ensure that there will be enough time for the action to be performed. The main point is that the analysts will have to provide a reasonable basis for the use of a time margin of less than 100%. Similarly, for the more unusual or challenging cases where the uncertainty may be greater, a good analysis of the time required will be important and the assumption of a larger time margin may be appropriate.

3.4 Calculation of HEP for time critical responses [5]

The identification of time critical responses depends on understanding the relationship of the time available (Ta), i.e., the time before the plant reaches some undesirable state, and the 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. This has typically been modeled using time reliability correlations such as the HCR/ORE [6]. The approach adopted by EPRI in EPRI TR-100259 [6] was to use the CBDT for non-time critical actions and the larger of the HCR/ORE or CBDT HEPs for responses for which the time margin was small.

The approach presented here is different from the EPRI approach in two important respects. First it represents the time available as a distributed parameter and second, it assumes that the HEP of an HFE should consist two parts: the HEP caused by the time uncertainties 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 function f(Tn) and Ta in its probability density 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.

Pt(Tn> *Ta)* = ∑Prob [(Tn > *Ta)* and *(Tn = Ta)]* = ∑P(Tn > *Ta)* •*P(Tn = Ta)*

$$= \int_0^{\infty} (1 - F_\tau)(f_T \, \mathrm{d}t)$$

[5] EPRI's position is that while conceptually there is some merit in this approach, further research is needed before it is considered for widespread application. For example, the approach presented here does not distinguish between variability in the timing due to the unmodeled randomness in the plant conditions associated with a PRA scenario and uncertainty in determining those times. In the current time-reliability correlation approaches variability in the time available is typically addressed by choosing a bounding value that minimizes the time available. This, in addition to addressing variability, obviates the need for addressing uncertainty in that value. The extent to which adopting this new method may require changes to developing PRA scenarios has yet to be determined.

In summary, IDHEAS treats the time factor from four aspects: When the system time available for a HFE is less than the time needed to perform the human actions, the HFE is considered as not feasible and the HEP is assumed to be 1.0; Otherwise, the uncertainties in both the time available and time needed contribute to the overall HEP of the HFE and the contribution is calculated as the convolution of the probability distribution functions. Third, even though the time available is adequate for the HFE, operators may feel the pressure to get the action done as fast as possible in some scenarios; the time pressure may increase the likelihood of human errors. The effect of time pressure on HEP is considered in the decision trees of IDHEAS quantification model. Lastly, in the quantification model, the failure of a critical task can be credited for recovery only when there is adequate time for recovery.

3.5 References

1. 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.
2. Nuclear Regulatory Commission (NRC) (2000). Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). (NUREG-1624, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission.
3. Wakefield, D., Parry, G., Hannaman, G., & Spurgin, A. (1992). SHARP1: A Revised Systematic Human Action Reliability Procedure. (EPRI TR-101711, Tier2). Palo Alto, CA: Electric Power Research Institute.
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. 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.
6. Parry, G.W, A. Beare, A.J. Spurgin, and P. Moeni, An Approach to the Analysis of Operator Actions in Probabilistic Risk Assessment, (1992), EPRI TR-100259, Palo Alto, CA: Electric Power Research Institute.
7. Kolaczkowski, A., Forester, J., Gallucci, R., Bongarra, J., & Lois, E. (2007). *Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire*. (NUREG-1852). Washington, DC: US Nuclear Regulatory Commission.

4 TASK ANALYSIS AND DEVELOPMENT OF CREW RESPONSE DIAGRAMS

4.1 Introduction

In the IDHEAS analysis process, this part of the analysis is performed for each HFE that has been identified and defined at a functional level (described in Sections 2.2.1 and 2.2.2 respectively) in preparation for the quantification of the HEP using the IDHEAS decision trees (Chapter 5). A human failure Event (HFE) is defined in the ASME/ANS PRA standard [1] as a PRA logic model element that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or an inappropriate action. As discussed in Chapter 2, the focus of IDHEAS is on HFEs that represent a failure of the operating crew to respond correctly to a plant upset condition, such as an initiating event, or the failure of an operating train of a support system. A typical HFE functional level definition includes the following:

a) The PRA scenario in which the HFE is modeled which defines the plant status and identifies the functional response required in response to this plant status,
b) Accident sequence (or plant status/upset condition) specific procedural guidance that specifies the required operator response (e.g., EOPs, AOPs, annunciator response procedures),
c) Identification of cues that alert the operators to the need for response and additional cues or other information required to determine and perform the response,
d) Accident sequence specific timing of cues and relevant information related to plant status,
e) The plant state or physical condition by which the operator action must be completed, and the corresponding time window (TW), and
f) The equipment (e.g., system or systems) the crew uses in order to achieve the functional goal and the way in which the equipment is to be used to achieve success (e.g., initiate injection using system X, perform depressurization).

Note that PRAs may include HFEs that represent failure to perform a non-proceduralized response. In this case, item b) would not be directly applicable; instead this would be replaced by documentation of the state of practice or skill of the craft that would lead to the recognition for the need for response and the expected method of response. The PRA scenario specifies the initiating event and the hardware and operator action events that led up to the demand for the operator action whose failure is represented by the HFE. The preceding failures and the success events are both relevant for the HRA since they provide the context for the operator action and influence the time evolution of the plant physical parameters. It is the context provided by the plant state that determines which procedure(s) is (are) in effect and also which cues are applicable.

Part e) of the HFE definition is converted for the HRA into a Time Window (TW), which is an estimate of the time available for a successful response. Items e) and f) together comprise the success criterion for the HFE.

The purpose of the stage of the analysis discussed in this Chapter is to perform and document a task analysis of the overall required response to identify opportunities for the plant operators to make an error as input to the quantification of the HEPs. Identification of these opportunities requires an identification and definition of the critical tasks in the performance of the response. A critical task is one that if not performed correctly will result in failure of the response. In the following, critical tasks are identified with the significant transition points in the response, such as entering a procedure, transitioning to another procedure, deciding to begin implementation, and execution. Success in performing a critical task may require the successful performance of one or more specific cognitive and manipulative activities such as collecting data, comparing

data to a decision criterion, and aligning a system for injection. Failure to successfully perform these activities leads to failure of the critical task and, therefore, results in the HFE.

In addition, following an initial failure to perform a critical task, the nature of the procedures may provide opportunities for the operating crew to recover from that failure within the time window for successful response, thereby avoiding the failure of the required mission. Included in the task analysis is the identification of opportunities for such recoveries.

The concept of a crew response diagram (CRD) has been developed for the purpose of communication, illustration, and documentation of the task analysis. The opportunities for both errors and for recovery are represented as nodes on the CRD as discussed below. In parallel, as an essential part of developing the CRD, a time-line (discussed further in Section 4.2.1) is developed that captures: a) the plant status trajectory in terms of the timing of cues and other plant process parameters that are required for the crew to correctly perform the required response or to realize an opportunity for recovery, and b) the time at which operators are expected to reach critical steps in the procedure.

If, at any stage in the development of the task analysis, it can be determined on the basis of any of the criteria addressed in Chapter 3 that the response is not feasible, the analysis of the HFE is terminated, and either the HEP is set to 1 or the HFE is removed from the PRA model. As an example, a detailed assessment of the task requirements may indicate that the manpower available to perform the response is not adequate. As another example, the specific HFE context may be such that the time needed by the operators to negotiate their way through the procedure would be too long for the response to be successful.

4.2 Task Analysis and Associated Timeline

4.2.1 Overview

The purpose of the task analysis is to understand what the crew has to do to achieve success. The individual tasks that, if failed to be performed correctly, result in failure of the overall mission, are identified as critical tasks. Other tasks, such as checks and verifications that, while not essential for success, are taken into account in the assessment of the time taken for the crew to navigate their way through the procedural path. For the purposes of a representation of results of the task analysis, a task may be defined at varying levels of detail. Ultimately this entails breaking down the tasks into the associated cognitive and execution activities since these are the links to the CFMs. Since there can be several critical tasks the individual tasks need to have clearly defined boundaries, such that each critical task has:

- A clearly defined goal
- A clearly defined initial or entry state
- A clearly defined ending or exit state (i.e., consequences or outputs)

The task analysis is performed via three main stages as shown in the following table and discussed in detail below.

Table 4-1. Overview of the task analysis stages

Task Analysis Stage	Overall Objective(s) of the Step	Principal Inputs	Output
Stage 1. Characterization of the expected procedural success path and identification of critical transition points (nodes on the CRD)	Describe the evolution over time of the scenario and the procedural path for the crew to successfully respond to the plant challenge.	• HFE definition as outlined in Section 4.1 • Relevant procedures and relevant cues and their timing • Discussion with plant operations staff to determine correct interpretation of procedures and priorities in dealing with plant conditions. • PRA scenario T/H analyses	• Expected path through the procedures (entry, transfers, and sequence of procedure steps) • Identification of critical transitions (CRD nodes) • Chronology of significant events including: - arrival of cues - time by which response is to be complete (e.g., system time window Tsw)
Stage 2. Identification and detailed definition of critical tasks	Identification of the critical tasks associated with the steps of the procedure or as determined from standard operating practice, that are required to successfully perform the transition represented by the node. Definition of the individual success criteria. Identification of the specific activities (e.g., collect information, such as check an indicator or trajectory of a cue [SG level] over time) underlying the critical tasks.	Same as above	• Understanding of the role of the steps in the procedure • Definition of critical tasks • Identification of critical activities, particularly activities associated with diagnosis of the need for a response such as transitioning to another procedure, selecting a response option, or initiating a system (the tasks). • Definition of requirements for success for each of the contributing activities • Detailed chronology of events including: - Time to reach relevant procedural step - Time to complete critical tasks - Contribution of non-critical tasks to the timeline - Assessment of manpower that supports the timeline

Stage 3. Identification of Recovery Potential	Identification of the opportunities for correction given failure at one of the nodes identified in Stage 1 or 2, and the requirements for successful recovery.	• Expected operator behavior (e.g., path being followed through the procedures) given failure to perform a critical task. Note that a critical task will fail due to the failure of one of the critical activities. • Procedural guidance and relevant cues and their timing. • Skill-of-craft or other recovery opportunities determined from standard operating practice, including relevant cues and their timing.	• For each of the critical tasks identified in Stage 1 or 2, identification of an opportunity for error correction, and a definition of what is necessary for recovery, e.g., additional cues and or/procedural directions that are relevant to the failure path. • Incorporation of recovery paths on the CRD

Note that while the crew tasks listed in the success criteria documented in the functional HFE definition provided by the PRA analysts may typically include solely the manipulations to be performed, the implementation of IDHEAS requires in addition the identification of activities associated with critical information collection, cognitive activities such as interpretation and decision, and the associated procedure-following activities. These will be discussed further in the description of the various stages of the task analysis.

Timeline

The development of a timeline is performed in parallel with the task analysis. The evolution of the plant status parameters developed as part of the PRA scenario definition provides the information necessary to identify the time at which cues are received, the plant status at the time each critical step in the procedural path is reached, and the time by which the responses must be completed. The time required for the crew to successfully proceed through the identified success path and the time required to reach and follow a recovery path are developed through discussion with operations staff and simulator observations.

One purpose of the timeline is to support assessment of the feasibility of the response and once the response has been determined to be feasible, to assess the feasibility of the identified recovery path. The timeline is also critical to the characterization of the failure scenarios that will be identified during the application of the quantification approach. The timeline is intended to capture the crew response, so aspects of the context, such as sufficiency of manpower, influence of distractions and prioritization of actions, are implicitly assessed in the construction of the timeline as the timeline must consider who-does-what-when. Guidance on the factors to be taken into account when considering feasibility and assessing the time required for the operators to perform the response is included in Chapter 3, and may be used whenever the analyst determines it is appropriate to do so. In general, however, the feasibility assessment will be performed after the details of the expected scenario have been worked out in developing the CRD and the timeline has been developed. An example timeline is presented in Section 4.4.5. In the following, the focus is on the identification and characterization of the critical tasks and activities and development of the CRD.

4.2.2 Stage1. Characterization of the Expected Procedural Success Path

4.2.2.1 Objective of Stage 1

The objective is to understand and characterize the expected success path for the required response in the context of the evolution over time of the PRA scenario, and to identify the correct path at decision points in the procedure, and any transitions between procedures. These decision and transition points are critical in that if any of them is failed, the response will fail. They may be thought of as the highest level of definition of a critical task.

4.2.2.2 Stage 1 Analysis

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

- **Identification of the procedures 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, checklists, etc.) that guide the crew. The procedural guidance for interpretation and decision-making that leads to the crew's selection of a response to execute may be separate from the procedural guidance for executing the manipulations. This should have already been included in the HFE definition.
- **Determine the relevant cues and their timing.** Cues include alarmed, annunciated and prominent plant indications that call attention of the crew as well as plant indications that the crew must actively collect to determine the plant status needed to make the appropriate response. This is particularly important for cues that lead the crew to enter a procedure, or once in a procedure, to take a specific action. This requires a timeline to be constructed using thermal hydraulic calculations. The ordering of the occurrence of the various cues and other information determines the success path. This should already be determined from the definition of the HFE.
- **Confirm plant practices for implementing procedures.** Discussion with the operations staff is necessary to ensure that the plant practices with respect to implementing procedures are correctly interpreted. In some cases there may be more than one procedure that is necessary for successful response, and the approach to such situations (e.g., prioritization of sequential implementation, perform in parallel) needs to be understood to establish the appropriate CRD structure.
- **Identify trained responses of the crew that are relevant to the success path.** In some cases, an HFE may represent a response that is not guided by a written procedure, and may instead involve responses based on training or skill-of-the-craft. In addition, the method of response may include actions that are not specifically called for in the procedure. The identification of these aspects of response requires interviewing plant operations staff.

Additional Comments for Complex HFEs

For many of the HFEs typically included in internal, at-power PRAs, the identification of the procedural path, the construction of the CRD and its associated timeline is straightforward as the example included in this chapter demonstrates. However, scenarios that involve multiple failures, especially those involving failures in support systems, several procedures may be called into play, involving multiple and different responses. Defining the HFEs and constructing the associated CRD requires an understanding of the crew's priorities in addressing the relevant responses as instilled by training and plant operations practices. For these complex scenarios, the HRA analyst may need to make assumptions to choose a representative procedural path to be represented in a CRD. If there is uncertainty about the path that is likely to be chosen, the assumptions should be identified as being associated with a source of model uncertainty, and alternative representative paths analyzed as needed to understand the significance of the assumptions. An example of a complex example is included in Appendix A. In extreme or

unusual cases, the combination of plant signature, procedures and training may produce an expected path that does not lead to success; in those cases further assessment is not needed, the HFE should be set to 1.0 and that insight relayed back to operations.

4.2.2.3 Documentation of Stage 1

The outcome of this stage is a description of the expected crew response, to include the path taken through the procedures in terms of the path taken at any decision points or transition points within the procedures. This description takes into account the timing of the relevant cues and other plant status parameters that are relevant to determining the appropriate procedural response. In IDHEAS, the documentation of Stage 1 can be organized as a series of nodes along the top line of a crew response diagram (CRD) (e.g., see Figure 4.1. This specific example is discussed in detail in Section 4.4.).

There is some degree of flexibility regarding the number of nodes to include in this representation. For example, a node could be included for each critical task that is needed for success (as discussed below in Stage 2) or several critical tasks may be included in the definition of one response node. In the end, both approaches would result in the same assessment. However, for ease of communication, it is recommended to display the success path in terms of the high level tasks such as those that are associated with entry into a procedure, transfer to another procedure, jumping ahead to another step in a procedure, initiation of a response, or execution of a response.

It should be noted that the individual tasks associated with the physical manipulation of plant systems (i.e., activities associated with aligning and/or starting a system) by the crew are not represented in the CRD; instead, they appear in related groups as part of a node on the tree. See examples below in Section 4.4). This is done to be consistent with the approach taken to the assessment of the execution HEPs described in Chapter 5.

Following this approach therefore, each node represents a critical high level task on the expected success path. A failure to perform the critical high level task identified by the node represents a potential failure opportunity of the overall response, and is represented by a branch at that node; however, the failure paths are not examined at this stage (they will be treated in Stages 2 and 3). In addition to the response nodes, it is useful for communication purposes to include on the CRD information nodes indicating assumed successful operator responses (e.g., entry into E-0, transfer to ES-01), or the initiating plant condition requiring response (e.g., an initiating event, which in the figure below is the complete loss of feedwater).

The times at which relevant cues and other plant status parameters occur, and the time available for successful response are documented on the timeline.

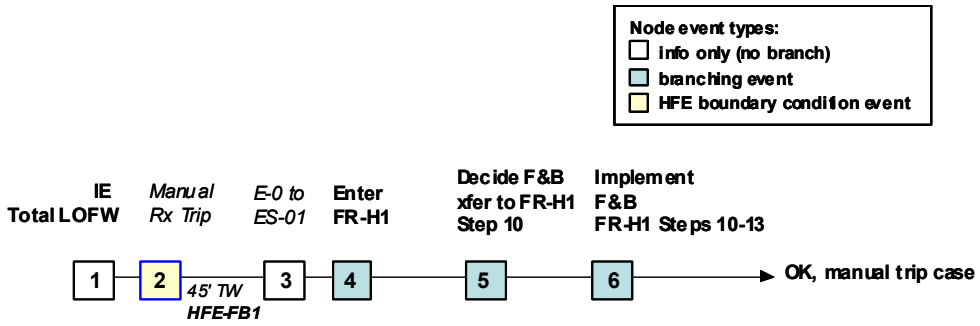


Figure 4-1. CRD expected success path

4.2.3 Stage 2. Identification and Detailed Definition of Critical Tasks

4.2.3.1 Objective of Stage 2

The purpose of this stage is to identify, for each node on the CRD, what the crew has to do to achieve success. This is done by first defining the critical tasks, and for each critical task identifying the specific cognitive and execution activities required for success. These activities include those related to data collection, comparing data against procedures, decision-making or response execution activities (e.g., aligning and initiating a system). For each activity, what is required to be successful is defined. This is an important step in the IDHEAS process because identifying the required activities is the link to identifying the applicable CFMs. This is discussed in detail in Chapter 6.

4.2.3.2 Stage 2 Analysis

In this stage, a detailed analysis of the steps in the procedure (or in the skilled responses for non-proceduralized actions) is performed. Individual steps in the procedure have different purposes, e.g., a step may direct the crew to collect information, to verify a plant status, to perform a plant status assessment, to make a decision such as transferring to another procedure or branch of a procedure, to execute the required manipulations, or they could even be included as precautionary measures to allow access during the recovery phase and restoration of the plant to service.

Once the role of the step in a procedure (whether written or learned) has been understood, the identification of those tasks that are essential for success is straightforward. Verification steps for example are not essential in the sense that if they are omitted they do not necessarily lead to failure of the task. However, they are important from the point of view of reducing the potential for error, and therefore they should be documented in the discussion of the relevant node. This information will be used during the quantification process later on. Similarly, when evaluating the time required for the crew to get to a point in the procedures as input to the feasibility analysis it should be assumed that such verification steps are taken since they may contribute to the time required.

For some procedural steps, particularly those related to establishing the plant status, the results of several information gathering activities may be required to be combined via a logic statement. This occurs, for example, when a number of plant parameters are assessed and the requirement for a transition is made on the basis of only one of the set of parameters (i.e. OR logic), or more than one the parameters (i.e. AND logic) being in the unfavorable range. At this stage, the activities associated with the assessment of each of the parameters need to be identified. How this is addressed in quantification of the HEP will be addressed in Chapter 6.

The characterization of each critical task should include the following, as this will be used later in the determination of which CFMs need to be considered (also see descriptions of example nodes and associated tasks in Section 4.4):

- Identification of the procedurals step(s) involved
- Clearly define the goal of the critical task (e.g., determine whether SI is required; transition to another procedure; etc.)
- Define the success criterion (e.g., determine if any one of 3 (specified) plant parameters is out of the specified range; determine all 3 (specified) plant parameters are outside the specified range; correctly interpret procedural direction to transition; etc.)
- The basic requirements for the task (e.g., obtain correct data; continuously monitor cues; use secondary cues when the primary cues are not available; respond to key alarms; implement the responses within a certain time window; etc.)

- Values of the plant parameters used to determine the correct response as determined from the T/H analyses. This is required to establish what the operators should see.
- Based on the above characterization of the critical task, the specific activities necessary for success are defined:
- For cognitive tasks, this includes the specific cognitive activities, such as detection of a cue, reading a control panel, interpreting a piece of information that has been actively obtained, comparing a plant parameter to some criterion specified in a procedure, choosing a response path.
- For execution, the specific manipulations that need to be performed, and their ordering if important.

Other information not directly used in the construction of the CRD includes:

- The crew member responsible for the activity
- Identification of needed tools, keys for access, keys for execution, etc.
- Where are the activities within the scope of the node performed?
- What interactions with other people are required to accomplish the task?

This information is however, necessary and will either be used when assessing the HEP as described in Chapter 6, or will have been an input to a feasibility analysis.

4.2.3.3 Documentation of Stage 2

The documentation of this step does not necessarily alter the appearance of the CRD, but instead it is used to define the nodes of the CRD so that the success criteria of the critical tasks and associated activities are defined. This will be used to define failure. Therefore, when constructing this representation, it is important to define clearly what procedural steps, and therefore the underlying cognitive activities, are required to be successful. For example, suppose the mission relies on a successful transfer to a procedure (e.g., FR-H1 in the example above). This may require success in collecting data guided by one procedural step, and processing of that data using the guidance in another procedural step. These activities are both included in the definition of the node "Enter into FR-H1". So, for the node "Enter into FR-H1", the associated activities would be data collection and comparison against a numerical criterion for two separate parameters:

- Monitor the CSF Status Tree for Heat Sink Success criterion and correctly determine that *neither* of these criteria is met
  - "NR Level in at least one SG GREATER THAN n1% [n2%]"
    - Data collection
    - Interpretation (comparison with numerical criterion)
  - "Total AFW Flow to SGs GREATER THAN n3 GPM"
    - Data collection
    - Interpretation (comparison with numerical criterion)

A structure for representing Stage 2 information for the nodes in Table 4.1 is presented in the illustrative example in Section 4.4.

As mentioned earlier, it is also possible at this stage to choose to represent each individual critical step of a procedure as a node on the CRD. So, for example, in this case, the node for a transition to the correct procedure could be expanded to represent individually the activity of obtaining specific pieces of information and the activity of using a criterion to determine the transition is necessary. At whatever level the branches of the CRD are defined, the same list of activities necessary for success would be derived. For example, in the CRD in Figure 4.1, "Decide F&B" (Node 5) and "Implement F&B" (Node 6) were separated into two separate nodes;

however, they could have been combined and represented as one node of “Decide and Implement F&B”. In either case, the same set of activities would result:

Representation 1

Node: Decide F&B (Evaluate the criteria listed in FR-H1 Step 2, entitled “Check secondary heat sink” and transfer to Step 10)

Activities: Correctly determine that neither of these criteria is met:

- “NR Level in at least one SG GREATER THAN n1% [n2%]”
  - Data collection (one-time check)
  - Data interpretation (compare against numerical criterion)
- “Total AFW Flow to SGs GREATER THAN n3 GPM”
  - Data collection (one-time check)
  - Data interpretation (compare against numerical criterion)

Node: Implement F&B (per FR-H1 Steps 10-13)

Activities:

- Step 10. Actuate SI
  - Execution (Actuate SI)
- Step 11. Verify RCS Feed Path
  - Data collection
  - Interpretation
- Step 12. Establish RCS Bleed Path
  - Data collection
  - Execution (manipulations to open the PZR PORVs)
- Step 13. Verify Adequate RCS Bleed Path.
  - Data collection
  - Interpretation

Representation 2

Node: Decide & Implement F&B (Evaluate the criteria listed in FR-H1 Step 2, entitled “Check secondary heat sink” and transfer to Step 10, then perform steps 10-13 to start F&B)

Activities:

- Correctly determine that neither of these criteria is met:
  - “NR Level in at least one SG GREATER THAN n1% [n2%]”
    - Data collection (one-time check)
    - Data interpretation (compare against numerical criterion)
  - “Total AFW Flow to SGs GREATER THAN n3 GPM”
  - Data collection (one-time check)

Data interpretation (compare against numerical criterion)

- Step 10. Actuate SI
  - Execution (Actuate SI)
- Step 11. Verify RCS Feed Path
  - Data collection
  - Interpretation
- Step 12. Establish RCS Bleed Path
  - Data collection
  - Execution (manipulations to open the PZR PORVs)
- Step 13. Verify Adequate RCS Bleed Path.
  - Data collection
  - Interpretation

This is important because the CFMs for quantification are evaluated at the activity level, and how the HFE is parsed should not affect the final analysis. In this section we have chosen to adopt the philosophy of using the nodes to represent significant transitions in the procedural paths, and have defined the critical tasks accordingly.

4.2.4 Stage 3. Identification of Potential Recovery Opportunities

4.2.4.1 Objective of Stage 3

Each of the critical tasks identified in Stage 1 represents an opportunity for failure. This is represented on the CRD as a downward arrow (Figure 4.2). The purpose of this stage is to explore the possibilities for recovery given a failure at one of the nodes of the CRD. 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 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. In Figure 4.2 it is assumed that these actions will succeed and therefore Node 3 in the Figure 4.2 does not include a failure path (branching point) and therefore recovery is not addressed.

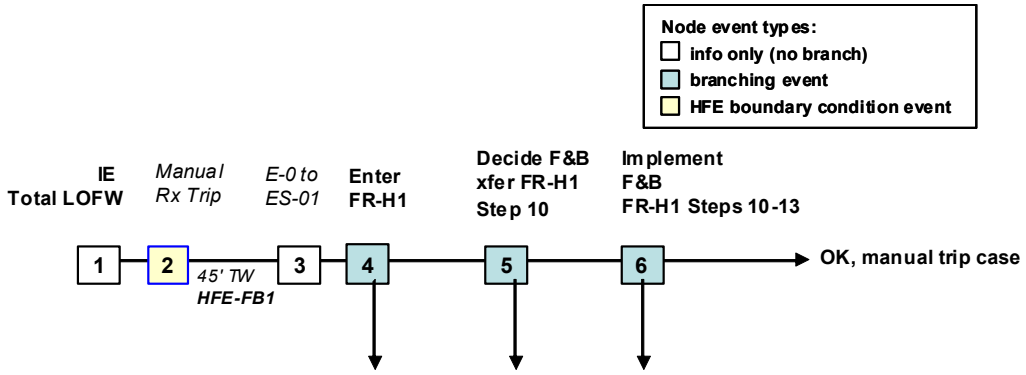


Figure 4-2. Opportunities for Failure

4.2.4.2 Stage 3 Analysis

The critical tasks represented in the CRD nodes include not only manipulations but also information collection, assessment and response selection tasks. The opportunities for recovery can come from a number of sources. Information collection, assessment and response selection tasks 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 reason for failure will be explored on a CFM basis when applying the decision trees as explained in Chapters 5 and 6), the assumption is made that following the failure to take the correct path that the operators are still using their procedures. Consequently, 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, plant 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 manipulation tasks, 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.

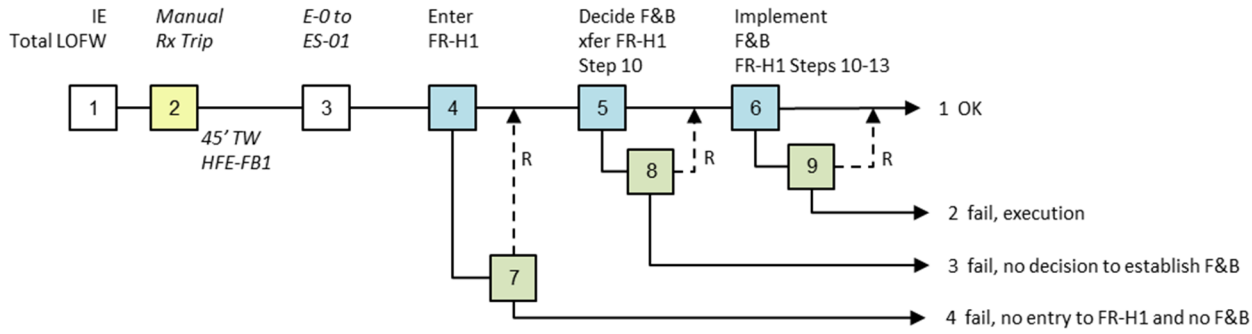


Figure 4-3. Error correction opportunities and their relation to the CRD expected success path

If opportunities are identified, they are represented as indicated in Figure 4.3, which shows a dotted line for recovery leading back to the success path. However, it is important to note that the recovery nodes, e.g., 7, 8, and 9 are not quantified separately. Rather, the recovery for a failure, for example, in node 4, is addressed within the DTs when quantifying the relevant CFMs for a given node. Thus, the recovery nodes 7, 8, and 9 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 on a CFM-specific basis when using the decision trees. 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. This is discussed in Chapter 5.

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 inappropriate as long as the analysts have a reasonable argument as to why they chose to model it the way they did, based on discussions with plant staff. 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.

4.2.4.3 Documentation of Stage 3

The completed CRD, an example of which is shown in Figure 4.3, provides a graphical representation for organizing the outputs of the task analysis. A summary of what is included in the CRD and the needed supporting information is in Table 4.2. A structure for representing the supporting information is presented in Section 4.4 in example form.

Table 4-2. Summary of the CRD documentation

Qualitative analysis outputs	Documentation
Expected success path.	The expected success path is described by listing the nodes along the top of the CRD (in Figure 4.3: these would be 1, 2, 3, 4, 5, and 6). Section 4.2.3.2 lists the types of information that would be provided for each of these nodes, including the identification and nature of the critical tasks. This information will be used to identify the CFMs that are relevant to the assessment of the failures. Example documentation is provided in Section 4.4.
Error correction opportunities (and associated performance factors) to be considered in the quantification of the CFMs.	The documentation of nodes 7, 8, and 9 of the CRD (see examples in Section 4.4) provides this information. However, note that, in quantification, recovery is addressed in the CFMs applied to nodes 4, 5, and 6 and nodes 7, 8, and 9 are not quantified separately.

4.3 Analysis of the CRD

The CRD is a representation of the ways that operators could fail to respond correctly in terms of critical tasks. The CRD also identifies potential correction opportunities.

The way this is used in the evaluation of HFEs is discussed in detail in Chapter 6. At this stage the feasibility of the recovery paths may be assessed. For example, if it can be established that the cues that could be used to correct a mistake would not occur before failure of the response then there is no opportunity for recovery. However, if the recovery is clearly feasible in that the cues for recovery would occur in time for diagnosis and recovery to the correct path, and time for the remaining tasks would also still remain available (e.g., any additional decisions or response execution activities), the assessment of recovery is addressed during the assessment of the relevant decision trees, because, as will be seen, the potential for recovery is dependent on the crew failure mode.

4.4 Example Demonstration of Task Analysis and Development of CRD

This Section provides an example task analysis and development of the CRD for a specific HFE, the failure to implement F&B in a Total LOFW scenario, given the reactor is manually scrammed on recognition of the loss of feedwater. For the scenario in which the reactor is not scrammed manually, but allowed to trip automatically, the HFE representing failure to implement F&B would be defined differently to reflect the fact that the time available to initiate feed and bleed would be considerably less. The reference plant is a Westinghouse 4-loop plant. The first section defines the HFE used in the example. Each of the subsequent three sections represents the task analysis at the end of Stages 1, 2, and 3 as discussed in the preceding sections of this chapter.

This example is a very simple one; further examples are provided in Appendix A to illustrate some of the more subtle aspects of the analysis.

4.4.1 Definition of the HFE Used in the Example

Item	For the HFE treated in the example
HFE identifier	HFE_FB1_TLOFW
HFE short description	Failure to implement feed and bleed (F&B) in a Total LOFW scenario
PRA scenario	Total Loss of Feedwater (TLOFW), followed by a manual reactor scram, and failure of the auxiliary feedwater (AFW) system, i.e. a complete loss of the heat sink.
Plant state or physical condition by which response must be completed / time window	In this scenario, F&B must be implemented to avoid core damage. The time window is 45 minutes.
Manipulations required for successful crew response	Implementation of primary F&B by actuation of Safety Injection and opening of both pressurizer (PZR) Pilot Operated Relief Valves (PORVs).
Equipment used to achieve functional goal	Feed is established using HHSI pumps. Bleed is established using the PZR PORVs.

4.4.2 Task Analysis Stage 1 Result – Characterization of the Expected Success Path

As discussed in Section 4.2.2, Stage 1 of the task analysis identifies the relevant plant cues and their timing, the applicable procedures in the scenario, relevant trained responses, and combines this information to establish the expected crew response and path through the procedures that will lead to success of the functional goal, in this case, establishing F&B in a TLOFW scenario.

At a high level, the expected success path for establishing primary feed and bleed (F&B) is the following sequence of crew responses:

1. The initiating event, total LOFW
2. Manual reactor trip and entry into the E-0, the post-trip procedure “Reactor trip or Safety Injection”
3. Transfer from E-0 to ES-01, “Reactor Trip Response”
4. Entry into FR-H1, “Loss of Secondary Heat Sink”
5. Decision to establish F&B and transfer to FR-H1, Step 10
6. Implementation of F&B per FR-H1, Steps 10-13

In this example, with the exception of the manual trip, events 2 through 6 are all critical for success. The manual trip is not critical because a trip would have occurred in any case. However, as discussed below, assuming a successful manual trip by the crew is an important boundary condition for determining the time available for successful initiation of feed and bleed. The expected success path can be graphically represented as a sequence of nodes, corresponding to the “main trunk” of a Crew Response Diagram (CRD), as shown in Figure 4.4. In Stage 1 Task Analysis, each of the nodes is then characterized at a high level, describing

- the plant cues and their timing
- the procedural steps (and, if applicable, crew trained responses) associated with this CRD event
- the manipulations performed

With the general scenario context and scope of the node thus described, Stage 2 Task Analysis will then decompose the nodes representing the critical tasks within the crew’s response into required activities and characterize these in detail.

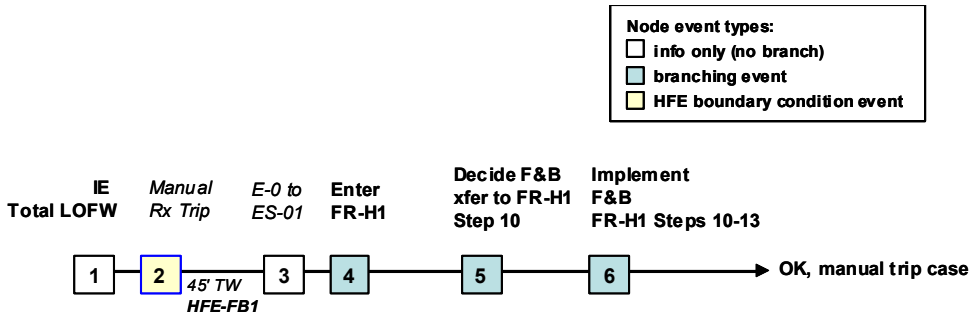


Figure 4-4. CRD expected success path (repeat of Figure 4.1)

4.4.2.1 Node 1 (Stage 1) – IE Total LOFW

The plant is initially in full-power operation. The main feedwater (MFW) pumps fail or trip. Auxiliary feedwater (AFW) pumps should start automatically, but in this scenario they fail to do so. The reactor will trip automatically on low-low SG level approximately 1 minute after the loss of feedwater.

4.4.2.2 Node 2 (Stage 1) – Manual Rx Trip

HFE-FB1 assumes that the operators will trip the reactor manually within 45 seconds of the loss of feedwater. If the reactor is tripped manually within 45 seconds, the time window (TW) for establishing F&B is 45 minutes.

In the case that the reactor trips automatically on low-low SG level, the TW for establishing F&B is substantially shorter; it is 13 minutes. This is due to the comparatively lower SG levels at reactor trip. The scenario with automatic reactor trip should be treated as a separate HFE.

Node 2 (stage 1)	
Label	Manual Rx Trip
Success outcome	The crew trips the reactor manually within 45 seconds of the Total LOFW
Crew response modeled by node	Perception of the cues resulting from the Total LOFW and manually tripping the reactor.
Operational narrative	The crew will perceive the FW alarms (MFW trip and alarms) and the rapidly decreasing SG levels.
Manipulations (Execution tasks)	Manual reactor trip.
Plant evolution and key cues for node	FW alarms (MFW trip and alarms), the rapidly decreasing SG levels, SG Low-Level Alarms, SG Low-Low Level Alarms.
Procedural guidance	The Entry Conditions to E-0 list the reactor trip criteria. The relevant criterion is SG LO-LO Level, 2/4 channels on 1/4 SGs Less than or equal to 20% NR.
Comment	Successful Manual Rx trip is assumed as a boundary condition for this HFE.

4.4.2.3 Node 3 (Stage 1) – E-0 to ES-01

Node 3 (stage 1)	
Label	E-0 to ES-01
Success outcome	Transfer to ES-01 at E-0 Step 4 and begin monitoring of the Critical Safety Functions using the Critical Safety Function Status Trees (CSFST)
Crew response modeled by node	This node models the crew response from reactor trip to the transfer to ES-01 and the monitoring of the critical safety functions at E-0 Step 4.
Operational narrative	In this scenario, the crew will check plant indications. There are no required manipulations in the scope of this node. In E-0 Step 4, they decide that SI is not required and are then

	instructed to transfer to ES-01, which guides the response to reactor trip when SI is not required and begin monitoring of the Critical Safety Functions, .
Manipulations (Execution tasks)	Not applicable.
Plant evolution and key cues for node	(Cues and information for the immediate response to reactor trip, beginning with control rod “bottom lights”, position of turbine valves, etc.)
Procedural guidance	Steps 1 to 4 of 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. These are essentially memorized steps that are well practiced.
Comment	This task is assumed successful, but this node is included on the expected success path to a) characterize the initial tasks of the crew, b) remind analysts to include the time to perform these tasks within the overall evaluation of time margins.

4.4.2.4 Node 4 (Stage 1) – Enter FR-H1

Node 4 (stage 1)	
Label	Enter FR-H1
Success outcome	The crew enters FR-H1
Crew response modeled by node	This node models the crew response from ES-01 entry to the entry into FR-H1, while in ES-01. [NOTE: In this plant the only direct path that will instruct entry into FR-H1, “Response to Loss of Secondary Heat Sink” is via the Critical Safety Function Status Tree (CSFST) for Heat Sink. In other plants, procedures E-0 or ES-01 may provide another entry opportunity, and can be identified as an opportunity for recovery.] , The CSFST for heat sink instructs entry into FR-H1 when SG Levels are all below n1% NR and Total AFW flow is less than n3 gpm. (The criteria in the procedure specify the actual values n1 and n3, which are not shown in this example.)
Operational narrative	In E-0, the crew established that SI is neither actuated nor required. Since success had been assumed for step 4 in E-0, the crew is assumed to have successfully transferred to ES-01 and begun monitoring the CSFST. Monitoring the CSFST is primarily the responsibility of the STA. The plant parameters for SG NR Level and AFW total flow to the SGs indicate that the criteria for the “red path” are met. This is the condition in the Heat Sink CSFST for entering FR-H1. ES-01 deals with RCS Temperature (Step 1), FW status (Step 2), and whether there is either MFW or AFW to each of the three SGs (Step 3).
Manipulations (Execution tasks)	Not applicable Note: Concurrent to the monitoring of the CSFST, the crew will try to establish AFW flow to the SGs per step 3 of ES-01. These are not critical tasks for the success of the crew response because the successful response is based on the SG levels and the AFW flow rate indications, but, if successful, would obviate the need for F&B. For this example HFE, this success path is not viable.
Plant evolution and key cues for node	SG NR Levels, AFW Flow Rates. Additionally, the CSFST is automatically monitored (by a computer).
Procedural guidance	Critical Safety Function Status Tree for Heat Sink. ES-01 Steps 1-3. ES-01 Addendum 6 and Addendum 7 (for establishing MFW and AFW, respectively). Note: The Conditional Information Page for ES-01 and the steps of ES-01 do not include any condition for transferring to FR-H1.
Comment	In the expected success path, the crew enters FR-H1 while following procedure ES-01. However, it is important to note that the criteria for entering FR-H1 are not part of ES-01. The instructions and goals of ES-01 may be viewed as competing with the monitoring of the CSFST and may potentially interfere with the interpretation and decision-making relative to the CSFST criteria, or later, the implementation of feed and bleed.

4.4.2.5 Node 5 (Stage 1) – Decision to Initiate F&B and Transfer to FR-H1 Step 10

Node 5 (stage 1)	
Label	Decision to initiate F&B and transfer to FR-H1 Step 10

Success outcome	The crew transfers to FR-H1, Step 10, the first step in establishing RCS F&B.
Crew response modeled by node	This node models the crew response from entry to FR-H1, “Loss of Secondary Heat Sink” to the decision to establish F&B. This decision and transfer to FR-H1 Step 10 is expected to occur at FR-H1 Step 2.
Operational narrative	The crew enters FR-H1 because it has determined previously that there is a Loss of Secondary Heat Sink. Step 1 of FR-H1 verifies whether Secondary Heat Sink is required while Step 2 is a check of Secondary Heat Sink. In FR-H1 Step 2, the crew determines that the criteria are not satisfied (SG WR level and PZR pressure) and follow the “Response Not Obtained” instructions to trip the RCPs and transfer to FR-H1 Step 10. Note: The crew may try to establish AFW flow to the SGs per FR-H1 Step 3, although it has not succeeded previously in ES-01.
Manipulations (Execution tasks)	Not applicable.
Plant evolution and key cues for node	SG WR Levels PZR Pressure
Procedural guidance	In this scenario, the guidance for the decision to initiate F&B is expected to be FR-H1’s Step 2. The criteria for the expected response (left column of procedure) are SG WR Levels in at least 3 SGs GREATER THAN n3 %; Pressurizer Pressure LESS THAN n4 psig. If either of these criteria is not met, Step 2 “Response not obtained” instructs the crew to trip the RCPs and to go to (transfer to) Step 10.
Comment	Note: The decision to establish F&B in FR-H1 is not guided by Step 10. Step 10 is the first step guiding the initiation (implementation) of F&B. The decision to establish F&B is based on the criteria in FR-H1 Step 2; this step is entitled “Check Secondary Heat Sink”. The “same” criteria are then continuously applicable based on FR-H1’s Conditional Information Page although the CIP criteria are expressed as the inverse. This is modeled by node 8 of the CRD (figure 4.3), discussed below. However, since the same cues are used, this can be credited as a viable recovery path is arguable. It is shown here for completeness.

4.4.2.6 Node 6 (Stage 1) – Implement F&B per FR-H1, Steps 10-13

Node 6 (stage 1)	
Label	Implement F&B per FR-H1 Steps 10-13
Success outcome	Actuation of SI (HHSI) Opening of PZR PORVs
Crew response modeled by node	This node models the initiation of F&B as guided by FR-H1, Steps 10-13.
Operational narrative	The main steps to initiate F&B are Step 10. Actuate SI Step 11. Verify RCS Feed Path Step 12. Establish RCS Bleed Path Step 13. Verify Adequate RCS Bleed Path.
Manipulations (Execution tasks)	The manipulations, which are the critical manipulations for this HFE, are guided by FR-H1 Step 10 and Step 12. Steps 11 and 13 are verification steps.
Plant evolution and key cues for node	The key cues for this node are for monitoring the feedback of the system (rather than being cues for the required tasks). They include: - indication of HHSI pump running - many valve position indications (including flow path valves, PRZ PORV valves, PZR PORV isolation valves)
Procedural guidance	FR-H1, Steps 10-13, guides the initiation of F&B. A caution above FR-H1 Step 10, on the same page instructs the crew to perform Steps 10-13 “quickly to establish RCS heat removal by RCS bleed and feed.”

Comment	Note: The decision to establish F&B in FR-H1 is not guided by Step 10. Step 10 is the first step guiding the initiation (implementation) of F&B.

4.4.2.7 Critical Nodes of the Expected Success Path

The critical tasks of the expected success path are those associated with nodes 4, 5, and 6. The following table documents the rationale for this selection of critical tasks. Consequently, only nodes 4, 5 and 6 are addressed in Stage 2 of the Task Analysis.

CRT Node	Rationale for selection / exclusion as critical
1. IE Total LOFW	This is the initiating event.
2. Manual Rx Trip	This is a HFE boundary condition event. In this scenario, the crew is assumed to manually trip the reactor within 45 seconds.
3. E-0 to ES-01	The response to reactor trip per E-0 is highly trained and there are no factors in this scenario that would suggest an alternative response. (An alternative approach would be to include this as a critical task node and analyze it to demonstrate that the probability is negligible. This approach is illustrated in example 1 in Appendix A, section A.1.)
4. Enter FR-H1	**Critical Node.** This is the crew's decision that there is a Loss of Heat Sink.
5. Decision to initiate F&B and transfer to FR-H1 Step 10	**Critical Node.** This is the crew's decision to initiate F&B.
6. Implement F&B per FR-H1 Steps 10-13	**Critical Node.** This is the implementation of F&B, in which the manipulations required for success of the response addressed by the HFE are performed.

These critical nodes represent the opportunities for failure of the HFE, as shown in Figure 4.5.

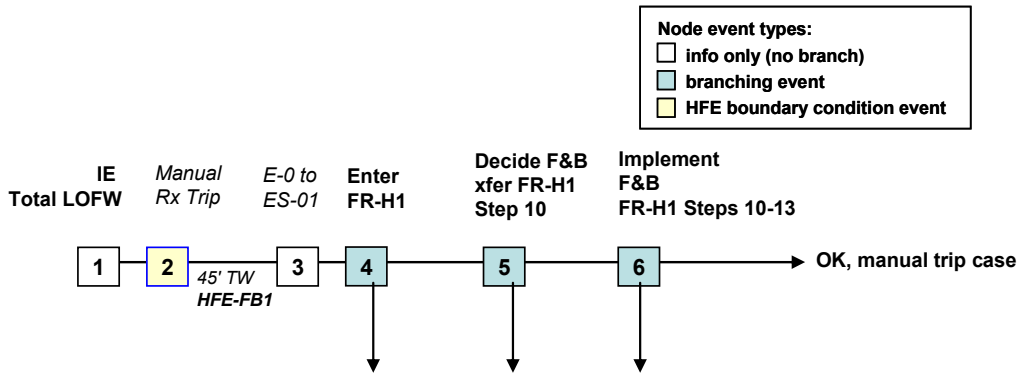


Figure 4-5. Opportunities for failures in the Task Analysis Example (repeat of Figure 4.2)

4.4.3 Task Analysis Stage 2 Result – Identification and Detailed Definition of Critical Tasks

In this stage, the critical tasks that comprise the expected success path are analyzed and characterized. The critical tasks associated with the critical nodes (4, 5, and 6) are broken down into critical tasks and their associated cognitive activities.

4.4.3.1 Node 4 (Stage 2) – Enter FR-H1

Node 4 (stage 2)	
Label	Enter FR-H1
Success outcome	The crew enters FR-H1
Crew response modeled by node	This node models the crew response from the time of entry into ES-01 to the entry into FR-H1 during ES-01 Step 3. As noted previously, it is the Critical Safety Function Status Tree (CSFST), monitoring of which is concurrent with entry into ES-01 that will instruct entry into

	FR-H1, “Response to Loss of Secondary Heat Sink”, when SG Levels are all below n1% NR and Total AFW flow is less than n3 gpm.
Operational narrative	In E-0, the crew established that SI is neither actuated nor required. In such a case, they transfer to ES-01. ES-01 deals with RCS Temperature (Step 1), FW status (Step 2), whether there is either MFW or AFW to each of the three SGs (Step 3). Per the CSFST, the crew needs to monitor the plant indications for SG NR Level and AFW flow and determine that the criteria for the “red path” are met. This is the condition for entering FR-H1.
Manipulations (Execution tasks)	Not applicable Note: The crew will try to establish AFW flow to the SGs. These are not critical tasks for the success of the crew response, but if they were to be successful would obviate the need for feed and bleed.

* All information from Stage 1 is relevant to the Stage 2 characterization of the node. To avoid excessive repetition in the stage-by-stage presentation of this example, solely the entries above are shown. They provide the background information for the discussion of the critical activities below. In an actual analysis, all of the information would be carried forward.

In the following, the critical tasks are described, and the activities required to perform those critical are identified.

Critical Task (Node 4 stage 2)	Nature of activities required	Characterization and further information
Monitor the CSF Status Tree for Heat Sink Success criterion: Correctly determine that neither of these criteria is met: “NR Level in at least one SG GREATER THAN n1% [n2%]” AND “Total AFW Flow to SGs GREATER THAN n3 GPM”	For both the narrow range level and total AFW flow the activities are the same: Data collection Interpretation (comparison with numerical criterion)	Procedural guidance: The CSFST for heat sink is one page with a flow chart linking the criteria. Plant information used: SG NR Level indications and AFW Flow indications. Responsible crew member: STA Note 1: The criteria for selection of the CSFST path are objective criteria, requiring no additional judgment. Note 2: A correct assessment of both these indications is essential to reaching the red path on the CSFST. Note that all SGs levels will read low so the indications are reinforcing. Note 3: They are performed in parallel with performance of ES-01. In Steps 1-3 of ES-01, the control board operators (i.e., other than the STA) are attempting to establish MFW or AFW flow.

4.4.3.2 Node 5 (Stage 2) – Decision to Initiate F&B and Transfer to FR-H1 Step 10

Node 5 (stage 2)	
Label	Decision to initiate F&B and transfer to FR-H1 Step 10
Success outcome	The crew transfers to FR-H1, Step 10, the first step in establishing F&B.
Crew response modeled by node	This node models the crew response from entry to FR-H1, “Loss of Secondary Heat Sink” to the decision to establish F&B. This decision and transfer to FR-H1 Step 10 is expected to occur at FR-H1 Step 2.
Operational narrative	The crew enters FR-H1 because it has determined previously that there is a Loss of Secondary Heat Sink. Step 1 of FR-H1 verifies whether Secondary Heat Sink is required while Step 2 is check of Secondary Heat Sink. In FR-H1 Step 2, the crew determine that the criteria are not satisfied (SG WR level and PZR pressure) and following the “Response Not Obtained” instructions to trip the RCPs and transfer to FR-H1 Step 10. Note: The crew may try to establish AFW flow to the SGs per FR-H1 Step 3, although it has not succeeded previously in ES-01.
Manipulations (Execution tasks)	Not applicable.

	Note: The crew may try to establish AFW flow to the SGs, although it has not succeeded previously in ES-01. These are not critical tasks for the success of the crew response.

* All information from Stage 1 is relevant to the Stage 2 characterization of the node. To avoid excessive repetition in the stage-by-stage presentation of this example, solely the entries above are shown. They provide the background information for the discussion of the critical activities below. In an actual analysis, all of the information would be carried forward.

Note: In FR-H1, Step 1 is a check to confirm that a heat sink is required. If this step were missed it would not affect the success path. Since it is clear at this stage that there is no feedwater flow the likelihood of a negative response at this step is small. Therefore it is not considered a critical task in the sense defined previously. However, the time taken for the verification should be taken into account when assessing feasibility. Once the crew has transferred to the RNO column at step 2, the guidance there requires the RCPs to be tripped. However, successfully tripping the RCPs is not critical to the success of feed and bleed and therefore is not considered a critical task, but should be considered in the timeline.

Critical Task (Node 5 stage 2)	Nature of activity	Characterization and further information
Evaluate the criteria listed in FR-H1 Step 2, entitled "Check secondary heat sink" and transfer to Step 10. Success Criterion: Correctly determine that neither of these criteria is met: "NR Level in at least one SG GREATER THAN n1% [n2%]" AND correctly determine "Total AFW Flow to SGs GREATER THAN n3 GPM"	Data collection (a one-time activity) Interpretation (compare against numerical criterion)	Procedural guidance: The criteria are provided in a bulleted list in the left column (Action / Expected Response) of FR-H1 Step 2. The first criterion concerns SG WR Levels. The second criterion concerns Pressurizer Pressure. Plant information used: SG WR Level indications and PZR Pressure. Responsible crew member: (TBD) Note 1: The criteria are numerical, requiring no additional judgment. Note 2: In FR-H1 Step 2, the expected response is met (continue to Step 3) if both criteria are met and not met (transfer to RNO column) if either criterion is not met, i.e. AND-logic for the expected response to be met. This is consistent with the CIP criteria for RCS B&F, where the inverse criteria are listed explicitly as OR-logic. Evaluating the plant status is a critical step in the procedure that involves cognitive activities associated with assessing both SG levels and pressurizer pressure.

4.4.3.3 Node 6 (Stage 2) – Implement F&B per FR-H1, Steps 10-13

Node 6 (stage 2)	
Label	Implement F&B per FR-H1 Steps 10-13
Success outcome	Actuation of SI (HHSI) Opening of PZR PORVs
Crew response modeled by node	This node models the initiation of F&B as guided by FR-H1, Steps 10-13.
Operational narrative	The main steps to initiate F&B are Step 10. Actuate SI Step 11. Verify RCS Feed Path Step 12. Establish RCS Bleed Path Step 13. Verify Adequate RCS Bleed Path.
Manipulations (Execution tasks)	The manipulations, which are the critical manipulations for this HFE, are guided by FR-H1 Step 10 and Step 12. Steps 11 and 13 are verification steps.

* All information from Stage 1 is relevant to the Stage 2 characterization of the node. To avoid excessive repetition in the stage-by-stage presentation of this example, solely the entries above are shown. They provide the background information for the discussion of the critical activities below. In an actual analysis, all of the information would be carried forward.

Critical Task	Nature of activity	Characterization and further information
(Node 6 stage 2)		
The critical task is to implement feed and bleed using the following steps in the procedure:	Execution	Procedural guidance: FR-H1 Step 10 states “Actuate SI” (check whether this is a “one-button” operation or equivalent). It has no “response not obtained” criteria or instructions, all of which are addressed by Step 11.
		Plant information used: not applicable
Step 10. Actuate SI		Responsible crew member: (TBD)
		Note: this is a critical manipulation and part of the HFE success criterion.
Step 11. Verify RCS Feed Path	Data collection	Procedural guidance: FR-H1 Step 11
	Interpretation (compare to desired state, specified by procedure).	Plant information used: Indication of HHSI Pump running (not specified in procedure), Valve position indications for HHSI pump suction, HHSI pump discharge, and HHSI cold leg injection valves.
		Responsible crew member: (TBD)
Step 12. Establish RCS Bleed Path	Data collection Execution	Procedural guidance: FR-H1 Step 12 Plant information used: Indications of power to PZR PORV isolation valves, valve position indications for PZR PORV isolation and PZR PORVs.
		Manipulation: opening the PZR PORVs.
		Responsible crew member: (TBD)
		Note: this set of manipulations is critical and part of the HFE success criterion.
Step 13. Verify Adequate RCS Bleed Path.	Data collection Interpretation	Procedural guidance: FR-H1 Step 13
		Plant information used: The procedural guidance instructs the crew to check that the PORVs and PORV isolation valves are open. It is unclear whether this is by checking the position indication or a flow indication associated with the PORV.
		Responsible crew member: (TBD)
		Note: In IDHEAS, execution is addressed in an integral manner rather than by assessing each of the individual sub tasks, as would be the case when using THERP for example. The details are used to assess whether the execution is simple or complex and in addressing the relevant PIFs as explained in Chapter 5. Therefore, the complete set of manipulations is identified as a critical task.

4.4.4 Task Analysis Stage 3 Result – Identification of Recovery Potential

The critical tasks identified in Task Analysis Stage 1 correspond to opportunities for failure. Stage 3 of the Task Analysis identifies the recovery potential.

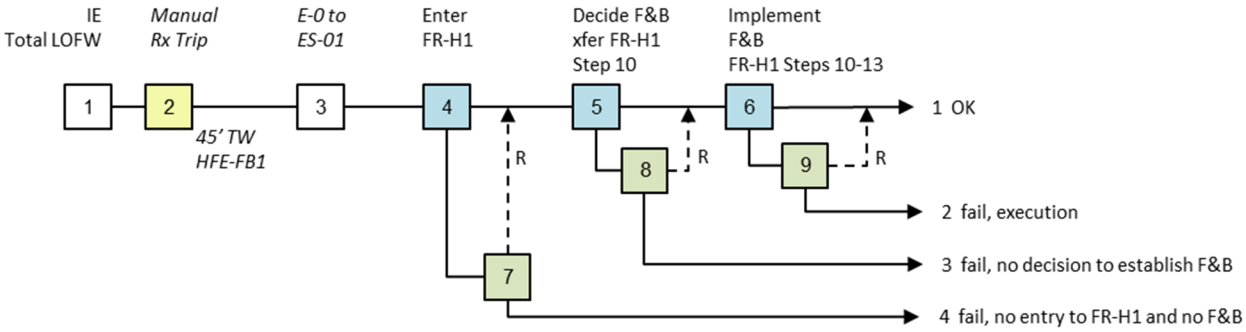


Figure 4-6. Error correction opportunities and their relation to the CRD (repeat of Figure 4.3)

4.4.4.1 Node 7 (Stage 3) – Recovery of Node 4 (Failure to Enter FR-H1)

Node 4 represents the critical task to enter FR-H1 as instructed by the CSFST, which is monitored after entering procedure ES-01. Node 7 represents asynchronous opportunities for recovery.

Node 7	
Label	Recovery of Node 4 (of the failure to enter FR-H1)
Failure of Node 4	Success of node 4 is based on the STA monitoring the Heat Sink CSFST, as required when ES-01 is entered and subsequently. The CSFST criteria (discussed in the Stage 2 analysis for node 4) are objective comparisons against numerical criteria, suggesting that if the STA is monitoring the CSFST, they will transfer to FR-H1. On the other hand, the crew may be taken up with the efforts to restore feedwater per ES-01, which is the procedure in effect in parallel with the monitoring of the CSFST.
Cues	SG narrow-range (NR) levels Total AFW flow
Procedural guidance	The Critical Safety Function Status Tree (CSFST) for Heat Sink will instruct entry into FR-H1, "Response to Loss of Secondary Heat Sink", when SG Levels are all below n1% NR and Total AFW flow is less than n3 gpm.
Recovery potential	The CSFST will be periodically monitored by the STA on entry to ES-01 (modeled in CRT node 3). CRT node 4 models the initial checking of the CSFST. Subsequently, the CSFST will be monitored periodically. In addition, while performing ES-01, if the crew establishes that they do not have an effective heat sink, they would communicate this to the STA, occasioning him to relook at the SG levels. Because, in this plant, there is not an alternative procedural path to enter FR-H1, this would be the only opportunity to take credit for recovery. If there were another path, e.g., directly from ES-01 or even E-0, this would provide an independent means that is a more significant path for recovery.
Comment	In this case, the recovery potential for Node 4 modeled by Node 7 is based on the information from the crew who are trying to establish FW flow. Node 4 models the initial check of the CSFST when entering ES-01. Node 7 models subsequent checks of the CSFST while in ES-01, e.g. if the crew subsequently determines that they cannot establish FW flow through the various means instructed by ES-01). Crediting this as a potential recovery would require additional justification because of the close relation between Node 4 and Node 7, which are based on the same procedural guidance being used at different times by the same crew member. However, an indication that the crew is unable to establish feedwater flow would lead the STA to check the SG levels. In other plants, where there are alternate procedural paths to enter FR-H1, this would be a more convincing opportunity for recovery.

4.4.4.2 Node 8 (Stage 3) – Recovery of Node 5 (of failure to transfer to FR-H1 Step 10 for F&B)

Node 5 represents the critical task to transfer to FR-H1 Step 10 as instructed by the Response Not Obtained instruction of FR-H1 Step 2. Node 8 represents the recovery potential provided by the FR-H1 Conditional Information Page. The first condition addresses RCS B&F Criteria and instructs the crew to transfer to FR-H1 Step 10 if the criteria are met.

Node 8	
Label	Recovery of Node 5 (of the failure to transfer to FR-H1 Step 10 for F&B)
Failure of Node 5	Success of node 5 is based on the crew determining that the criteria in FR-H1 Step 2 are not satisfied (SG WR level and PZR pressure) and following the "Response Not Obtained" instructions to trip the RCPs and transfer to FR-H1 Step 10.
Cues	SG WR levels PZR pressure
Procedural guidance	The conditional information page of FR-H1 is applicable when in FR-H1. The first condition to be monitored is "RCS B&F Criteria After Step 1". The criterion is 'SG WR Levels on any 2 SGs LESS THAN n1% [n2%] OR pressurizer pressure GREATER THAN OR EQUAL to nnnn psig due to loss of secondary heat sink.] The crew should transfer to FR-H1 Step 10 when either criterion is satisfied.
Recovery potential	While in FR-H1, FR-H1's Conditional Information Page is applicable. The first condition listed in the CIP is "RCS B&F Criteria After Step 1". These criteria are the inverse of the criteria as listed in FR-H1 Step 2. (FR-H1 Step 2 provides criteria for adequate heat sink; if these are not met, the Response Not Obtained is applicable and instructs the crew to transfer to FR-H1 Step 10 to initiate F&B.) The CIP criteria are the criteria for establishing RCS B&F. Operationally, the crew will check the B&F criteria in FR-H1 Step 2 (modeled by Node 5); the CIP instructs them to continue to monitor these plant parameters throughout FR-H1 if the crew did not determine that the criteria were met in FR-H1 Step 2. In effect, the CIP indicates that the B&F criteria in FR-H1 Step 2 remain continuously applicable while in FR-H1. Furthermore, even if the crew does not transfer directly to Step 10, they will eventually get there by proceeding through the steps. As long as the time taken to reach Step 10 by this route is greater than the time window, this is also a potential path for recovery. However, the cues are the same and so the argument for recovery is not strong.
Comment	Note: The FR-H1 Step 2 criteria are equivalent to the FR-H1 Conditional Information Page "RCS B&F Criteria" but expressed inversely (The Step 2 criteria are listed as criteria for (adequate) heat sink while the CIP criteria are listed as B&F criteria; they are logically equivalent.) If the crew fails to go to Step 10 for some reason even when the criteria in FR-H1, Step 2 are met, then the potential for recovery exists based on their continued checking of the relevant parameters as guided by the CIP.

4.4.4.3 Node 9 (Stage 3) – Recovery of Node 6 (Failure during implementation of F&B)

Node 6 represents the critical tasks to establish RCS F&B as guided by FR-H1 Steps 10-13. Node 9 represents the recovery potential within these steps.

Node 9	
Label	Recovery of Node 6 (failure during implementation of F&B)
Failure of Node 6	Node 6 consists of the critical manipulations for this HFE and the verification that the manipulations establish feed through safety injection in the cold leg and bleed through the PZR PORVs.
Cues	Indication of HHSI Pump running (the specific indication is not specified in procedure) Valve position indications for HHSI pump suction, HHSI pump discharge, and HHSI cold leg injection valves.
Procedural guidance	FR-H1 Step 11 verifies that feed is established while Step 13 verifies that bleed is established.

Recovery potential	FR-H1 Steps 11 and 13 are intended to address the crew's failure to perform any of the required manipulations (as well as addressing the failure or misalignment of the equipment required for F&B).
Comment	Establishing RCS B&F is specifically guided by Steps 10 and 12 while Steps 11 and 13 represent the verifications that the plant has responded appropriately to Steps 10 and 12. So recovery credit is supported by the verification steps and the cues noted above. The assessment of recovery potential for execution is addressed in IDHEAS, directly by the decision trees as discussed in Chapter 5.

4.4.5 Timeline for the Example HFE

The timeline is developed between the Identification and Definition of the Critical Tasks and associated activities (Stage 2 of CRD development) and Identification of Potential Recovery Opportunities (Stage 3). In practice, there will be some iteration between the CRD development stages and timeline development.

The timeline is shown as a table in Table 4.3. The estimated durations refer to the time elapsed between either a) the occurrence of the plant cue (plant event) or b) the completion of the previous event until the task shown and the completion of the crew tasks. The estimated durations shown in the timeline represent the largest durations expected, in other words, they correspond to the performance that could be expected of the slowest crew or crews in this situation. The scope of the crew response for which the durations are being estimated are supported by the Stage 1 and Stage 2 CRD documentation. The Stage 1 documentation focuses on the scope of the crew response for which the duration is being estimated. For the critical tasks, the Stage 2 documentation provides a detailed breakdown of the activities.

Table 4-3. Timeline for the example HFE

Time (elapsed)	Estimated duration *		Crew response / Key plant events
T=0		Plant event	Total LOFW (initiating event, node 1)
45”	45s	Crew resp.	Manual Rx Trip (CRT node 2). Crew enters E-0 immediately after the manual trip at 45s. (The duration accounts for the perception of the cues resulting from the Total LOFW until the crew manual trips the reactor.)
5’	4 mins.	Crew resp.	Perform E-0 “immediate actions” and continue until the crew transfers from E-0 to ES-01 at E-0 Step 4. (CRT node 3) Note: the time stamp is rounded to the nearest minute value.
7’		Crew resp.	STA arrives after approx. 5 minutes after being called shortly after reactor trip (1 minute after reactor trip).
13’	6 mins. (after STA arrival)	Crew resp.	Enter ES-01 and begin monitoring the CSFST. Determine that the criteria for the “red path” of Heat Sink CSFST are met, which they will be for this scenario as determined by the PRA scenario definition and the associated T/H analysis. Under this condition, the CSFST instructs the crew to transfer to FR-H1. (CRT node 4) The crews would be expected to enter ES-01 at latest 5 minutes after the reactor trip (i.e. at T=6’). However, the duration of interest in this part of the response concerns the monitoring of the CSFST, the determination of the Heat Sink status (that there is a Loss of Heat Sink), and the decision to transfer to FR-H1. As noted in the documentation of this node, the performance of ES-01 may compete with the CSFST monitoring although the latter is the responsibility of the STA while the crew focuses on the former.
17’	4 mins.	Crew resp.	Entry to FR-H1, “Loss of Secondary Heat Sink”. Performance of initial steps in this procedure until FR-H1 Step 2. Guided by Step 2, the crew decides to establish F&B and transfers to FR-H1 Step 10, which guides the initiation of F&B. (CRT node 5).
25’	8 mins.	Crew resp.	Implement F&B per FR-H1 Steps 10-13. (CRT node 6).

Given the 45-minute time window estimated for this HFE, this timeline indicates that there are approximately 20 minutes available for recovery of failures or delays that occur during nodes 4, 5, and 6.

The example analysis of this HFE is continued in Section 6.3, where the outputs of the task analysis, in the form of the CRD and its supporting documentation, are used in the quantification of the HFE.

4.5 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

5 HRA QUANTIFICATION MODEL

5.1 HRA Quantification Model – Concept

The quantitative approach is a cause-based approach. The HEPs are assessed on the basis of explanations of why the HFE might occur (e.g., crew dismisses relevant information that results in their failure to achieve the required response). These explanations are informed by and consistent with the work done to identify cognitive mechanisms (e.g., bias), the consequences of those mechanisms (proximate causes of failure – i.e., a phenomenological description of the way the error is manifested such as dismissing relevant information), and the characteristics of the performance influencing factors (PIFs) that enable those mechanisms to result in errors (e.g., for the PIF "training", a specific characteristic relevant to bias could be the focus of the training on a scenario with a different but similar signature) [1]. In addition, since there may be opportunities for the crew to correct an error within the time window for success in response, these explanations also address whether and why such an recovery opportunity is feasible or not. The explanations are called ***crew failure scenarios***.

The crew failure scenarios are grouped in terms of the characteristic crew failure mode (CFM) as explained. For each CFM a decision tree (DT) is created. The branches of the DT represent the PIFs that have been determined to be relevant to determining the likelihood of the CFM occurring. Each path represents a different combination of the status of the PIFs, and represents a high level description of a crew failure scenario. The set of paths through all of the DTs represents, at the level of the PIFs, the complete set of crew failure scenarios represented in IDHEAS. As discussed in Chapter 6, depending on the nature of the response addressed by the HFE, it may be necessary to address several CFMs, and, to evaluate the HEP, a crew failure scenario will be associated with each CFM.

Which path through the DT is chosen for a specific HFE is determined by the specific characteristics of those PIFs that are determined by the context for the HFE. Thus in documenting the crew failure scenario for a particular CFM, the analyst will not only identify the path through the DT, but also the specific PIF characteristics that dictated the choice of that path.

Based on the set of CFMs and their associated DTs, the quantification of the HEP for the HFE takes the following form for a PRA scenario S:

$$HEP(HFE|S) = \sum_{critical\ tasks} \sum_{CFM} Prob(CFM\ |CRD\ sequence, S)$$

where the outer sum is over the CRD sequences that leads to the HFE, and the inner sum is over the CFMs that are relevant for the CRD sequence. The term $Prob(CFM\ |CRD\ sequence, S)$ is the probability associated with the end point of the path through the DT for the specific CFM that is determined by the assessment of the relevant contextual factors associated with the HFE (and the CRD sequence). The use of this model to evaluate the HEP for an HFE is discussed in Section 6.2.4.

5.1.1 Crew Failure Modes (CFMs)

To make the model tractable, the crew failure scenarios are grouped into *categories* labeled crew failure modes or CFMs. The 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. IDHEAS classifies human failures in relation to the cognitive tasks performed by a crew to achieve task goals. Any crew response is composed of a set of these cognitive tasks. Therefore, these CFMs represent the ways in which failures to perform those tasks or activities that are typically found in operating procedures

(whether written or learned) or standard operating practices could be observed to have occurred.

The CFMs are based on the generic cognitive tasks in crew responses performed in procedure based, PRA defined internal event actions. One basic requirement for defining CFMs is that 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 most generic cognitive tasks are not independent, i.e., the success of a task depends on preceding tasks, the CFMs need to be defined against artificial boundaries to each other in order to be non-overlapping. The description, or the words used to characterize the CFM, represents the common feature of the crew failure scenarios included in that category since it describes the failure mode in the crew failure scenario. If this initial failure is allowed to persist (i.e., is not recovered) the crew will fail the task in the PRA logic model (i.e. P(HFE|CFM)=1). What differentiates the crew failure scenarios in the same CFM category is the existence or absence of PIF characteristics that affect the likelihood of occurrence of the CFM. The PIF characteristics determines the DT path to obtain the HEP for a given CFM.

This representation is similar to the modeling of hardware. For example, the ways in which a pump might fail (fails to start, fails to run) are modeled, but the different causes of the failure of a pump to start are not modeled; however, some of the “PIFs” that affect the pump failure probability (e.g., type of medium (dirty vs. clean), type of pump, etc.) might be included by identifying different sub-populations of pumps with their own failure probabilities.

The CFMs were chosen by identifying potential failure modes of the various types of activities that can be identified for the procedure or experience driven crew interactions in Nuclear Power Plants (NPPs) internal at-power events, e.g., collecting data, comparing data with a criterion to determine what action to take, manipulating equipment. The set of CFMs represents a set of generic failure modes for these types of activities. From the cognitive perspective, the crew response and interaction with the plant can be represented within three phases: plant status assessment (SA), response planning (RP), and plan execution (E); the success of each phase depends on the success of the preceding phases. In addition to the three phases, communication is a cognitive function that supports the cognitive tasks in all of the phases. Crews perform a series of cognitive tasks within each phase; the success of a task depends on the success of the tasks preceding it. Crews also perform certain types of cognitive tasks throughout all of the phases, principally following procedures and monitoring critical parameters. These tasks are necessary to support and achieve success in all three phases.

Which CFMs are relevant for a specific HFE depends on the activities that are essential to the correct response. These activities are identified during the construction of the CRD and are either represented as nodes on the tree, or as critical tasks related to those nodes. Not all the generic types of activity will be relevant for an HFE; for example, for some responses there is no reliance on an alarm. In that case, for that HFE, the CFM related to alarms will not apply. In addition, the way in which these activities are performed affects which CFMs are relevant, e.g., if the data collection is a one-time activity, then CFMs related to monitoring are not relevant.

The primary source for determining CFMs was the cognitive basis structure developed through cognitive literature studies [1]. The cognitive basis structure identified the cognitive processes for the four basic cognitive functions (detection, understanding, decision-making, action execution, and teamwork) and the cognitive mechanisms that make the processes work. Cognitive mechanisms as described by [1] are analogous to the systems analysis concept of “failure mechanism,” in that they describe the means by which a failure mode can occur. The elements in the process for a cognitive function are basic cognitive activities. For example, for

success in the Detection function, the cognitive process for human actions in internal at-power events involves basic activities such as attending to cue sources, and perceiving and understanding the cue. Proximate causes (PCs) represent failures of the elements in the cognitive processes. For example, the PC of "cue/info not perceived" is the failure of the activity "Perceiving and recognizing the cues," an identifiable cause of failing to notice a cue or problem (i.e., failure of the detection function).

Our principle for identifying CFMs is to construct a set of non-overlapping CFMs that are the behaviorally observable representations of the PCs for procedural, internal at-power events. The behaviorally observable representations of the cognitive functions are referred to crew response phases: the Detection and Understanding functions together constitute the situational assessment (SA) phase, the Decision-making function corresponds to the Response Planning (RP) phase, and the Action function correspond to implementation or execution phase. For each phase, we then identified a set of basic cognitive tasks for crew responses in procedure based, internal event actions. These basic tasks represent the PCs but not necessarily in a one-to-one fashion; several PCs may be merges into one cognitive task or one PC may be split into several basic cognitive tasks in order to describe behaviorally observable crew responses. Appendix C describes the justification for these basic tasks and their relationships to the PCs. The basic tasks identified for procedural, internal at-power events are summarized as follows:

SA Phase:

- Identify and verify critical data
- Attend to the identified data source
- Perceive the data from the source
- Use the data to form assessment
- Continue to collect data to assure the assessment

RP Phase:

- Interpret procedures
- Choose appropriate strategies

Execution phase:

- Determine the timing of implementation
- Monitor parameters for initiating execution
- Initiate execution
- Execute simple or complex actions

In addition, there are two types of cognitive tasks associated with all the three phases:

- Attend to alarms (interpreted as detecting, understanding and correctly responding to the alarm)
- Follow procedures

The failure of each of these basic cognitive activities corresponds to one CFM distribution of CFMs within these phases is shown in Table 5-1.

Table 5-1. Crew failure modes (CFMs) within the phases they represent

Crew Failure Mode	Phase of Response			Comments
	Plant Status Assessment	Response Planning	Execution	
AR: Key Alarm not Attended to	Yes	Yes	Yes	A special case that covers recognizing the alarm, understanding it and taking the appropriate action.
SA-1: Data Misleading or not Available	Yes	-	-	
SA-2: Wrong Data Source Attended to	Yes	-	-	Wrong data source attended to during execution is included in execution CFMs.
SA-3: Critical Data Incorrectly Processed/Misperceived	Yes	-	-	Wrong data source misperceived during execution is included in execution CFMs.
SA-4: Critical Data Dismissed/Discounted	Yes	-	-	
SA-5: Premature Termination of Critical Data Collection	Yes	-	-	
RP-1: Misinterpret Procedures	-	Yes	-	If a contributor to the execution, it is included in the assessment of the HEP for execution.
RP-2: Choose Inappropriate Strategy	-	Yes	-	
E-1: Delay Implementation	-	-	Yes	
E-2: Critical Data not Checked/Monitored with Appropriate Frequency	-	-	Yes (miss cue to begin execution)	
E-3: Fail to Initiate Execution	-	-	Yes	
E-4: Fail to Execute Simple Response Correctly	-	-	Yes	
E-5: Fail to Execute Complex Response Correctly	-	-	Yes	
AP-1: Misread or Skip Critical Step(s) in Procedure	Yes	Yes	Yes	If a contributor to the execution, it is included in the assessment of the HEP for execution.
C-1: Miscommunication	Yes	Yes	Yes	Provided to aid the analyst in assessing ways in which communication may be affected; however, full quantification of this tree is not provided.

5.1.2 PIFs and Development of Decision Trees as the Basis for HEP Quantification

The CFMs, i.e., the various types of failure 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 loss of vigilance, lack of attention, or memory overload. The breakdown of cognitive mechanisms are 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. Most existing HRA methods typically model high-level PIFs including the following:

- Time available
- Task complexity
- Workload
- Human—System Interfaces (HSI)
- Procedures
- Training / knowledge
- Experience
- Work process
- Stress
- Fatigue (fitness-for-duty)

The Cognitive Basis Structure provides the inferences of links between CFMs, cognitive mechanisms, and 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. To quantify the HEPs of a CFM under different PIF status, we constructed a decision tree (DT) to represent the status of the PIFs: The tree consists of a set of branch points and branches; every PIF is represented with a branch point and two branches, nominal and poor; a DT path for a CFM represents one combination of the nominal or poor status of the PIFs. We also refer to a DT path as a failure scenario because it represents a type of scenarios that may lead to a CFM and thus the HFE.

In IDHEAS for internal at-power events, a decision tree (DT) was constructed for each CFM to provide a framework for estimating the failure probability of the CFM. The branch points within each DT correspond to the PIFs considered most relevant to the cognitive mechanisms that can result in the CFM. The concept behind this form of the quantification model is that it will prompt the analyst to assess the existence and “strength” or relevance of those factors affecting each CFM. The information concerning these factors is determined from the outputs of the scenario analysis, operational narrative development, context analysis , which are inferred from the definition of the PRA scenario (typically plant conditions, procedural guidance, timing information), or by review of operating practices, details of the procedures, the nature of the training and experience, etc. (the more traditional PIFs), or both.

The primary source for determining what PIFs were applicable for each DT was the Cognitive Basis Structure [1]. However, other PIFs were included as well if considered important through expert opinion and experience. The Cognitive Basis Structure [1] identified mechanisms that can lead to failure of a cognitive function. For use within IDHEAS, the mechanisms were identified as potential causes of observable errors within a system perspective (i.e., what is represented by the CFMs). The aim in identifying the CFMs, DTs, and ultimately the branch point questions in evaluating the context within the DT was to translate the cognitive mechanisms identified in the psychological space to the CFMs / DTs representing the plant

space. This mapping was necessary to identify the relevant PIFs associated with the cognitive mechanisms so that DT branch point questions could be developed.

The process in developing the DTs began by reviewing the links of the proximate causes (PCs), cognitive mechanisms, and PIFs in the Cognitive Basis Structure. Each cognitive mechanism associated with the chosen PC was then examined and each PIF associated with the selected cognitive mechanism was evaluated for its relevance to the DT based on expert opinion. The judgment for the relevance is constrained to the assumptions about internal at-power events (i.e., the assumptions about the HFEs in internal at-power events, including procedural actions in control rooms, performed by crew well trained on procedures and the HSI). The judgment is also constrained to whether the PIF can be assessed in a predictable manner. This eliminates some PIFs that can be poor in specific events as revealed by SDP/ASP but cannot be predictively assessed in general PRA models. This selection process is detailed for each DT in Appendix B. Deciding whether the PIF should be included was a process of examining each one and making a determination as to whether the PIF could influence the occurrence of the CFM. If the PIF was deemed to be appropriate for the CFM, it was included as a potential contributing factor.

Since the PIFs were inferred from cognitive mechanisms, it was possible to identify the explicit, observable, assessable characteristics of the high-level PIFs that are most relevant to a cognitive mechanism and the CFM. For example, lack of attention is a mechanism contributing to the CFM "Key Alarm Not Attended to;" the Cognitive Basis Structure identified HSI as a PIF that challenges the mechanism. Based on our experts' understanding of NPP control room design and work process, it was identified that alarm salience is the HSI characteristic causing lack of attention and increasing the likelihood of the CFM; therefore, we use "Alarm Salience" instead of HSI as a branch point in the DT for the CFM. Also, as multiple PIFs may lead to a similar observable effect with regards to the CFM, multiple high-level PIFs may be represented with one branch point in a DT. . For example, the branch point inquiring about the crew's familiarity with the data source in the DT for "Wrong Data Source Attended to" is meant to capture the PIFs of training, experience, and knowledge. the purpose of the branches on the DT is to elucidate those observable factors that may cause the CFM, and are, therefore, closely related to the high-level PIFs, but do not represent a one-to-one mapping of the high-level PIFs.

Once the critical PIFs were identified and categorized into branch points, questions were developed to address the specific characteristics of the PIFs that had an impact on human performance given the context of the tasks we were anticipating having to address. The questions used to assess the status of the PIFs addressed by the branch points were developed by identifying the task requirements associated with the CFM and identifying what human vulnerabilities may fail the identified task requirements. These vulnerabilities were converted (and possibly aggregated) into the operational context represented by the branches. The specific questions developed at the branch point were developed through expert judgment (with PRA and plant experience) as being pertinent to assessing the status of the PIFs. Although the specific questions asked at each branch point within the DT are meant to represent possible human vulnerabilities, the branch points are actually presented in operational terms that can be easily associated to plant operations, so some amount of translation had to be done in constructing the questions.

In addition to the branch points that assess the existence or absence of critical PIF characteristics, some DTs also include a branch related to the potential for recovery from the human error captured by that CFM. The considerations related to this recovery branch are focused on determining whether the conditions are such that recovery is both feasible and likely.

The actual construction of the DTs followed the following philosophy. If the characteristics associated with the PIFs assessed at the branch point are conducive to good performance, the down direction is taken at the branch point. However, in order to take the down direction, the conditions related to the PIFs must be nominal (i.e., no identifiable negative PIF characteristics), otherwise the up branch is taken. In general, Nominal can be equated to Good, since that is the expectation. The up branch is taken even if only one of the specific PIF characteristics is less than optimal. The implications of this are that the model cannot distinguish between those cases where only one characteristic of the branch point is bad and those where several characteristics within that branch point could be bad (i.e., only one or more than one question for the particular branch point has been answered in a negative manner). When using the model in a qualitative way, this is not a significant issue since the PIF characteristics that are negative can be readily identified, and proposed solutions are determined if required. However, this one-size-fits-all approach can be criticized from a quantitative point of view because it equates a scenario with one negative PIF characteristic to one that has several negative characteristics. Since doing anything more would lead to an explosion in the size of the DTs, this proposed approach has been adopted as a compromise between practicality and discriminatory power. Given that the scenarios in which several PIF characteristics are negative are probably in the nature of what are called deviation scenarios in ATHEANA [2], their frequencies are expected to be low and, therefore, this potential conservatism should not be a significant detriment to the use of the PRA in decision-making.[6]

The questions provided with the DTs to determine the PIF characteristic were developed as a reasonably complete set to assist the analyst in deciding the presence of negative characteristics. However, total completeness is an illusory concept. Therefore, the analyst should perform a reasonableness check when evaluating the branch points to rule out the presence of a negative PIF characteristic that may not be captured with the included questions.

5.1.3 Workload factors

The Cognitive Basis Structure identified workload as a PIF that contributes to most proximate causes (so to most CFMs). The workload as a PIF actually encompasses other high-level PIFs including time availability, task complexity, and fatigue. In HRA, when workload is considered a poor influencing factor, it means that the task demand relative to the crew's available cognitive resources is so high that it challenges human's cognitive capacities and leads to breakdowns of cognitive mechanisms. We developed a set of workload factors as summarized below:

- W1 – 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 as compared to familiar scenarios. In unfamiliar scenarios, the situation-specific tasks may not be explicitly identified in the procedures but rather need engineering judgment.
- W2 – Intermingled 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.

[6] This statement will need to be confirmed during the piloting phase of this method.

- W3 – 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 where operators are distracted/interrupted for a prolonged period of time (e.g., longer than 2 minutes) or interrupted by cognitively demanding tasks and requests.
- W4 – 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 change in a short time that require the operator to constantly monitor 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.
- W5 – Cognitive complexity: Cognitive complexity refers to the task demand for cognitive resources. Since the cognitive functions involve different processes, each function has its indicators of complexity.
- W6 – 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 extensive 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.
- W7 - Mental fatigue: Mental fatigue can be caused by long working non-routine, stressful hours, or performing unfamiliar, cognitive 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. Human tends to use heuristics (short-cut) in situation assessment and decision-making.

Each workload factor affects a different set of cognitive mechanisms thus different factors may contribute to different CFMs. We used specific workload factors rather than the high-level PIF "Workload" in the DTs.

5.1.4 Estimation of HEPs of DT paths

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 [5]):

- 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."

Given that human error data for HRA is very limited, and actuarial data about the specific CFMs and failure scenarios are essentially unavailable, we used expert judgment to obtain the HEP distributions for DT paths. The project team adopted the expert judgment method developed by the Senior Seismic Hazard Analysis Committee (SSHAC). 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.

The expert judgment panel we used consisted of total 16 experts (cognitive psychologists, PRA/HRA analysts, NPP operators / trainers); the experts were assigned specific roles, namely to: provide supporting technical information (e.g., regarding the details of operational experience and PRA/HRA analyses); provide (and defend) probability estimates; integrate the various expert estimates; and review both the execution of the elicitation process and its results. In accordance with the fundamental principles established by the SSHAC, the elicitation was aimed at developing probability distributions representing the state-of-knowledge of the informed technical community, and not just that of the expert panel. The panelists estimated the HEP distribution of DT paths, i.e., the likelihood that the context implied by the path through the DT results in the crew failure in that failure mode. The estimations by individual panelists were integrated to form the consensus HEP distribution. Appendix D documents the process of expert judgment.

The HEP distributions obtained through expert judgment are presented in Appendix D, at the end of this report. To use these probabilities, it is important to understand the assumptions made for eliciting expert judgment:

1. The HEPs are for critical tasks in a HFE, not for individual procedure steps;
2. The HEPs are for critical tasks in HFEs performed in control rooms by trained crew in internal at-power events;

3. The “Nominal” status of the PIFs are the expected conditions (e.g., experienced crew, well-trained procedures, well-designed HSI) and is typically associated with the GOOD choice, while the “Poor” status of PIFs represents the situation that the PIF is significantly deviated from the expected condition and challenges crew performance to the extent of failing the task;
4. The HEPs are for average crew.

5.2 CFMs and DTs for internal at-power events

This section describes the CFMs and their associated DTs. For each CFM, we first provide the definition of the CFM, followed by a discussion of its applicability. The discussion focuses on the scope of the CFM and boundaries between the CFM and other CFMs. Next, the DT is described with the explanation of the PIFs. Each PIF is accompanied by a list of reference questions that help analysts to judge the status of the PIF. Note that the questions represent the authors’ assessment of the significant characteristics of each PIF as it relates to the occurrence of the CFM. However, they do not necessarily represent all the circumstances or aspects related to the PIF. Also, some questions may not be applicable to specific scenarios. Thus, answers to the questions are not the sole criterion to determine the status of a PIF. The questions aid but do not solely determine the status. Analysts are encouraged to use their own judgment to collect additional information as needed for a thorough assessment of the PIF status.

5.2.1 AR: Key Alarm Not Attended To

5.2.1.1 Definition of CFM

This CFM represents the failure to respond to a key alarm. A key alarm is one that is the first indication of the need for a response, and in this context it is considered to be unexpected. Furthermore, a key alarm is not necessarily a single alarm, but instead it could be multiple annunciators that form a recognizable pattern. It is expected that the response for a key alarm is well trained and essentially automatic. Failure includes both the failure to perceive the alarm and failure to understand the alarm.[7] For those alarms for which the response is memorized, simple, and ingrained (e.g., pressing the scram control on receipt of a scram alarm), this could also include the failure to act. In other words, there is no need to separately model the failure to execute, particularly if the control stands out in some way that makes it highly unlikely that an incorrect control would be chosen. For alarms that lead to entering a procedure (such as an alarm response procedure) any actions contained within that procedure (e.g., collecting confirmatory data or performing diagnostic checks, and specific actions) should be addressed separately using appropriate CFMs. Understanding the alarm, in this case, includes entering the correct procedure and failure results in not entering the correct procedure.

5.2.1.2 Applicability

This CFM is applicable to a task (e.g., a branch on the crew response diagram (CRD) associated with responding to an alarm) for which, for the HFE in question, the principal cue is an alarm and a failure to respond would lead to the HFE directly. With this understanding, this CFM applies to HFEs where:

a) The alarm is the principal cue and is sufficient for a correct assessment of the plant status so that the required response is unambiguous for a nominal situation. The response is typically an immediate action (including pulling out a procedure) where there’s really no

[7] Note that if a critical alarm is disabled, this should be reflected in the boundary conditions for the HFE and the HFE would be given a conditional probability of 1.

decision to be made once the alarm has been registered (attended to). In the case of a key alarm, “not attended to” encompasses “not perceived”, “misperceived”, and “dismissed” (in contrast to the active search where these different failure modes are addressed separately), as well as failure to understand what the alarm means and perform the initial response. In this sense it is similar to the annunciator response model of THERP. These different failure modes could be modeled separately, but given that the types of alarms that are addressed in this category are expected to initiate an immediate response, it does not seem to be necessary.

OR

b) The alarm is a trouble alarm that leads to entry into an alarm response procedure. In a PRA model this can occur for HFEs related to response to the failure of a support system such as component cooling water (CCW) and service water (SW), for example. Such HFEs may, for example, be included in fault trees used to estimate the frequency of an initiating event resulting from a loss of a support system. Since equipment status alarms require the crew to use the appropriate alarm response procedure (and picking up the wrong procedure would be a failure to understand the alarm), and these usually require additional data gathering to determine the cause of the alarm and the appropriate response, it is assumed, for these cases, that additional information is needed to form a correct assessment of the plant status in order to correctly identify the response that is needed. The search for this additional information is a directed search, and may be directed by procedure or by skill-of-the craft supported by training and experience. Therefore, in analyzing an HFE that involves the search for additional information, the appropriate CFMs related to active data gathering would also apply as well as those related to response planning and execution.

This CFM does not apply to alarms that serve as reminders associated with parameters that are being monitored (e.g., low RPV level alarm, low CST level alarm), since these will generally be dealt with as recovery opportunities in other decision trees.

The CFMs SA-1 through SA-5 are for tasks involving directed search for data as opposed to responses to alarms , where detecting information is trigged by salient aural and visual signals, and where the need for response is unexpected. ,

5.2.1.3 Development of Decision Tree

The reasons for a key alarm not to be responded to are likely driven by cognitive overload, where the significance of the alarm is diminished by coincident alarms or other activities, and where the training and experience do not facilitate the crew’s ability to prioritize it correctly. The salience of the alarm itself is an important factor as is whether the control is clearly separated from and easily distinguished from other controls on the panel. The perceived urgency of the alarm, which is derived from knowledge/experience, is also a factor in successful response.

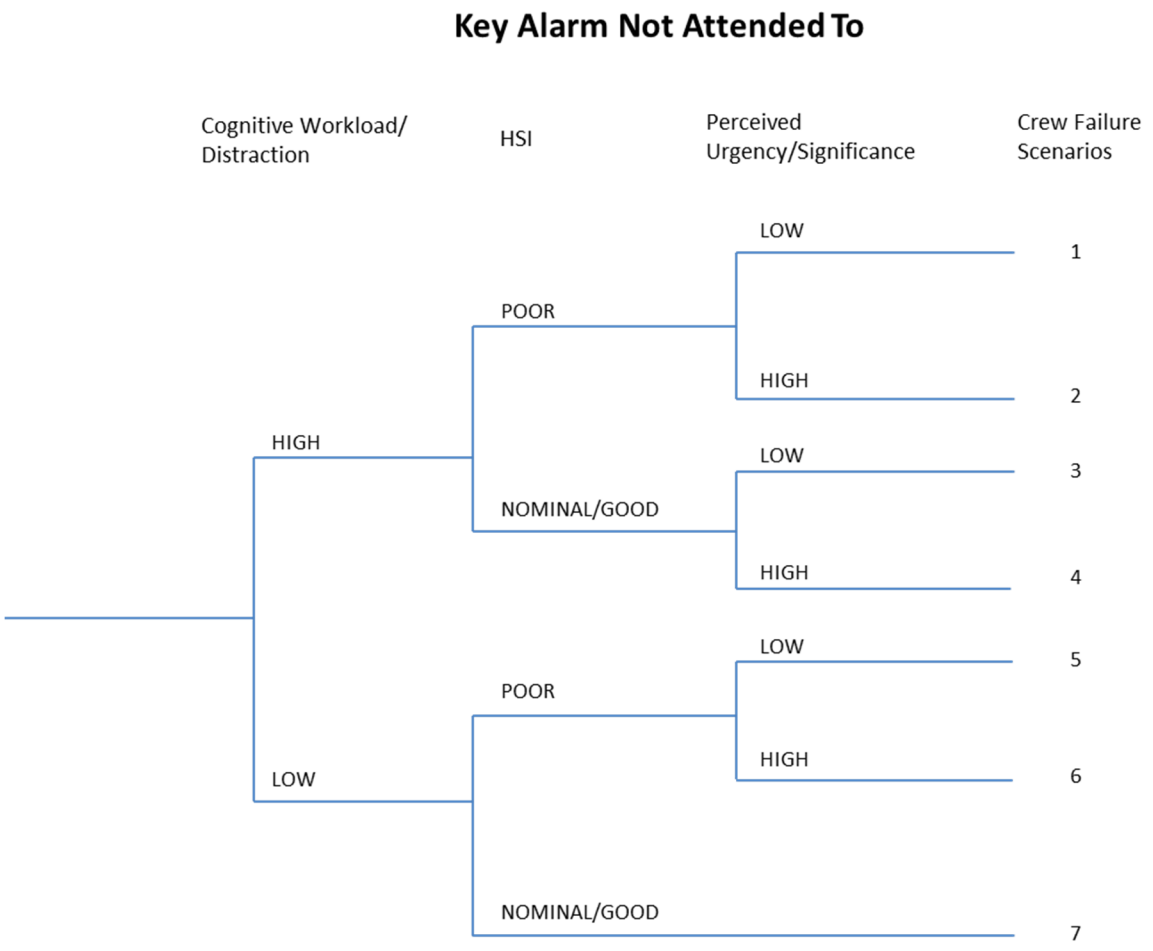


Figure 5-1. Decision Tree for CFM 'Key Alarm Not Attended To'

Branch Point 1: Cognitive Workload/Distraction

Definition: The purpose of this branch is to determine whether, for the PRA scenario, the cognitive workload is higher than that which is considered normal and for which operators are well trained. Distraction refers to non-critical or non-procedural tasks that compete for the operator's attention and other cognitive resources while the operator is performing critical tasks.

Explanation: One of the major reasons for missing an alarm is distraction. Distraction could result from a simultaneous demand for attention from other sources, which could be simultaneous unrelated alarms (plant status or equipment fault alarms) or the fact that the crew is already involved in performing other high priority tasks. The latter would be the case when the unexpected alarm occurs while the crew is attempting to respond to an initiating event and have not yet stabilized the plant. This branch point also addresses the perceptual issue of sensory overload (e.g., many unrelated alarms going off at the same time, not corresponding to a specific alarm pattern that the operators might be familiar with). However, it is necessary to understand what the normal alarm for this function would be, i.e., whether it is a pattern of alarms or a single alarm, and whether it typically occurs coincident with a number of other "alarms" that all require attention, but whose prioritization is established and understood.

Distraction here takes into account the balance between workload, manpower and time available. For example, if there is much going on, but there is sufficient manpower such that a dedicated person is available to monitor the relevant panels, then distraction would not be high.

Similarly, if there is high workload and limited manpower for the first 5 minutes, but the alarm persists for 20 minutes (i.e., the alarm persists to the point where distractions have been minimized) then there would not be a high distraction. This branch point is intended to address significant distractions, beyond what is nominally expected by the operators.

The following questions may be helpful in addressing this branch point:

a) For this PRA scenario, does the alarm occur coincident with other alarms that are unrelated to the function addressed by the subject alarm or when the operators must attend to multiple sources of information or tasks (other than as identified in the sentence preceding this paragraph)?
b) Does it occur at a time of high workload (e.g., while the operators are still in the process of determining the plant status, or while they are on the process of stabilizing the plant or restoring one of the key safety functions) such that the entire crew is occupied with specific response tasks?

➔ If the *either* of these is true, then the HIGH branch should be taken. Otherwise, the LOW branch should be taken. The LOW branch corresponds to there being nominal or minimal distraction present and is taken when the alarm is a solitary alarm, or if there are multiple alarms they are reinforcing in that they point to the same response. The HIGH branch, on the other hand, corresponds to competing alarms, or when the alarm occurs when the crew is preoccupied with other tasks.

Branch Point 2: HSI

Definition: The purpose of this branch is to distinguish between those alarms for which the HSI is potentially a negative factor, and those for which the HSI is nominal or good. This branch does not differentiate between nominal HSI and good HSI (i.e., where HSI would be considered a compensating factor for high distraction).

Explanation: When there are competing activities or alarms, the nature of the alarm may not be such as to demand attention. The issues addressed at this branch point are those related to the salience of the alarm; if it stands out clearly from other alarms and is unambiguous and when the response is a control board action and the target is clear and the manipulation straightforward and consistent with expectations, this would correspond to good HSI. However, if the alarm is obscured by its placement (e.g., on a back panel) or its design, or the scenario context is such that it leads to a failure to perceive the alarm, this would correspond to a poor HSI.

In addressing this branch point, the following questions may be helpful:

a) Is the alarm (or pattern of alarms) prominent, distinctive and unambiguous? Is the alarm or pattern of alarms discernible from the background noise generated by coincident alarms/information and is its relevance evident?
b) In the case that the response to the alarm is a physical response, can the target for response be unambiguously and readily identified, and is its manipulation consistent with practice (i.e., no non-stereo-typical or unintuitive actions)?

➔ If the answer to *either* of these questions is No, the POOR branch should be taken. Otherwise, the NOMINAL/GOOD branch should be taken.

Branch Point 3: Perceived Urgency/Significance

Definition: The purpose of this branch point is to determine whether the training and knowledge of the crew in the specific scenario is strong enough to compensate for distractions caused by high cognitive workload (as defined above in Branch Point 1) or poor HSI and lead to them recognizing and prioritizing the response to this particular alarm.

Explanation: For really critical alarms, the training and experience can be such that they will focus attention on the alarm even in the case of significant distraction. The issue addressed in this branch point is whether the training and experience of the crew emphasizes the significance of the alarm and the required response such that the operators are conditioned to recognize and prioritize the alarm. This is true for both alarms designed to protect equipment (e.g., low lube oil pressure alarm on a diesel generator) and those that require immediate corrective action to restore a critical safety function.

In addressing this branch point, the following questions may be helpful:

a) Is the alarm or alarm pattern understood as being a critical alarm that must be dealt with immediately irrespective of other alarms?

AND

b) Is the response, whether it be pulling out a procedure or manipulating a control or controls without reference to a written procedure, clearly understood and trained upon?

➔ If the answer to *both* these questions is Yes, then the HIGH branch should be taken. Otherwise, take the LOW branch.

5.2.2 SA-1: Data Misleading or Not Available

5.2.2.1 Definition of CFM

The data that the operators would use as their primary cue or source of information is misleading or is not available. This is essentially an HFE boundary condition governed by the system status so strictly speaking it is not a crew failure mode as such, but more a condition that would lead the crew to fail. It is included here for completeness since scenarios involving data unavailability or inaccuracy are not always included in a PRA model. This CFM is defined conditionally on the operators successfully knowing they need the information, i.e., they are in the correct procedure, and at the correct step in the procedure.

5.2.2.2 Applicability

This CFM is only invoked if the boundary conditions associated with the PRA scenario for which the HFE is being assessed are such that the primary data needed to form a correct plant status assessment (including a plant parameter [e.g., pressure, temperature, level, flow] or the status of a function, a system, or a component) is not available because:

a) Either the principal source of data is unavailable due to such things as instrumentation failure or scenario specific isolation of a critical instrument (e.g., the steam line from a ruptured steam generator is isolated so that the radiation signal does not indicate N16).

OR

b) The principal source of data is not indicative of the plant status because of additional equipment failures (e.g., a valve indicates closed even though it's leaking, or an open recirculation valve indicates flow through the system, even though there is a flow diversion so that the flow is not getting to the right place). These are examples of plant conditions masking the true nature of the plant.
These are external causes that result in the data required by the crew being unavailable or misleading. This DT addresses whether there are alternative means for obtaining the information, or an alternative means of establishing the correct plant status assessment. Given that scenarios such as the ones considered here are likely to have a low probability, this CFM may not be used frequently. However, it may be useful to understand the potential for recovery it addresses, particularly for the use of the model in a retrospective analysis of operational events. For PRAs that don't typically model instrumentation failures or indication

failures, this will only be invoked for deviation scenarios as they are referred to in ATHEANA [2].

This CFM is distinguished from the CFMs where data are obtained but dismissed, or the need for the data is understood and there is an intent to obtain it but it is not obtained in a timely manner (e.g., as a result of inappropriate sampling frequency). The failure scenarios for this CFM are conditioned on the unavailability of the correct data due to such things as instrumentation failure or scenario-specific isolation of a critical instrument. If this were the only way to get an indication of plant status, the probability of the HFE would be 1.0. Alternatively, if the procedure directs the crew to a contingency procedure because the data is unavailable or indeterminate, then this CFM does not apply. Instead, the relevant HFE is failure to perform the actions in the contingency procedure.

5.2.2.3 Development of Decision Tree

This decision tree addresses the likelihood of obtaining the necessary information to compensate for the unavailable or incorrect information. It questions whether there are additional information sources that can be used to supplement the incorrect or misleading data, whether the guidance or training would be such that this additional information is looked for, and whether that additional data would be sufficient to result in a correct plant status assessment. In that regard, using this decision tree relies less on the consideration of cognitive mechanisms than on understanding the HSI and work practices.

The first question to be asked is whether there is an alternate source to either contradict the misleading information or provide an alternate source to the unavailable data.

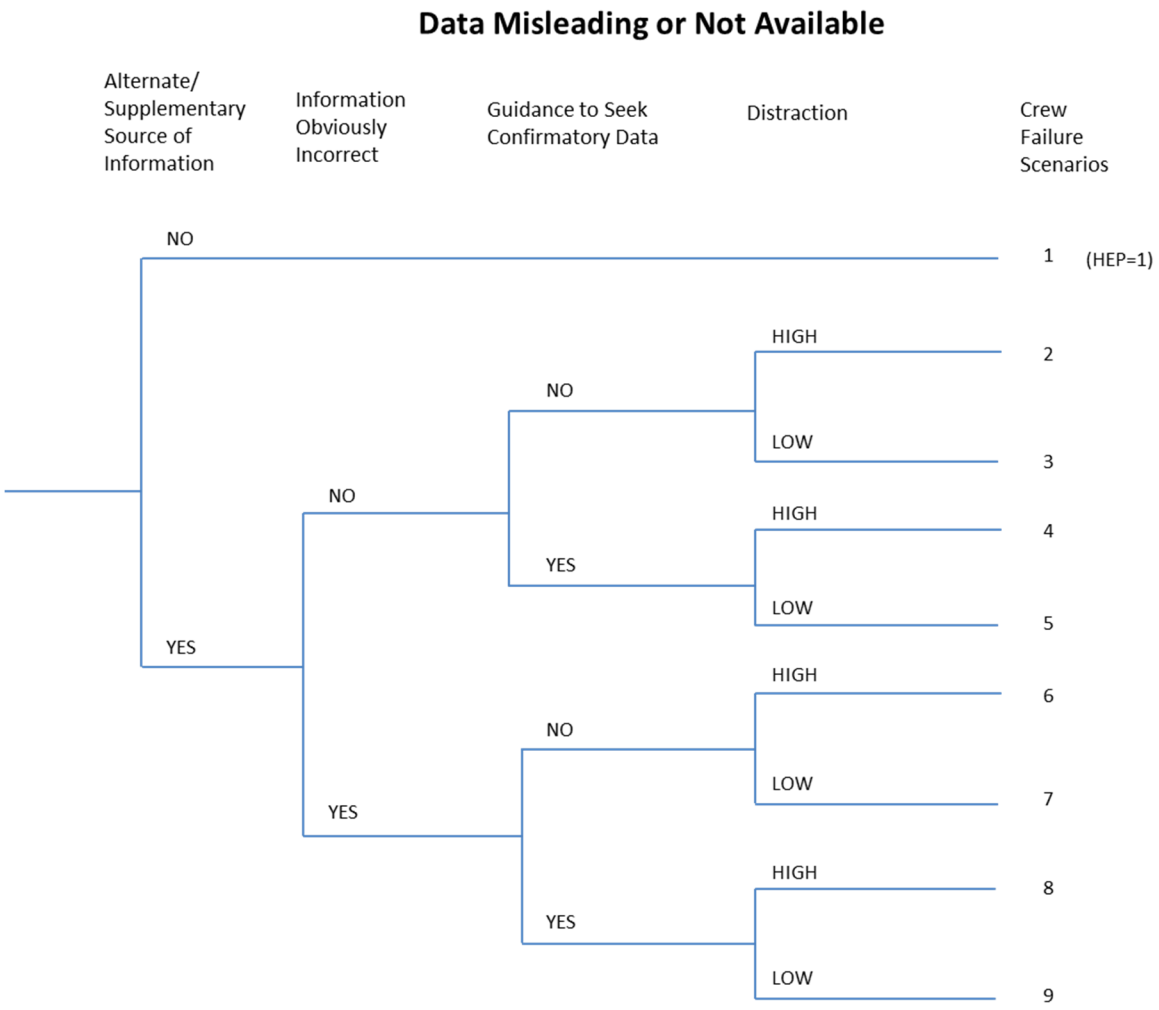


Figure 5-2. Decision Tree for CFM 'Data Misleading or Not Available'

Branch Point 1: Alternate/Supplementary Source of Information

Definition: This branch questions whether, given the primary cue or source of information is either failed or misleading, there are alternate indications that could be used to obtain the plant status. This is a screening question – if no viable alternative exists, the HEP defaults to 1.0. The remainder of the tree addresses the likelihood that the information will be obtained.

Explanation: The direction taken at this branch is determined by understanding whether there are any alternative or supplementary information sources available to the crew that can be relevant to determining the plant status. This requires the HRA/PRA analysts to understand the PRA scenario, including how and why the primary indications are failed. These information sources may be direct or, more likely, indirect indicators of the plant status. For example, if the primary data source is a level indicator on a tank and it reads steady, a supplementary or alternate source of data that provides an indication of flow into the tank could be used to conclude that there was a leak from the tank and that therefore the level indicator might be misleading.

The analyst searching for these sources should develop an understanding of the indications that are available and what they tell the operators about the status of the plant. Determining that there are indeed additional sources of data that could be used is a necessary prerequisite to addressing branch point # 3 on this decision tree: if no such sources can be identified, the presumption is that the crew has no option but to accept the information and therefore the HEP is 1.0.

In addressing this branch point, the following questions may be helpful:

a) Is there an alternate or supplementary source of information available to the crew that is both relevant to determining the plant status and relevant to the success of the response?

➔ If the answer to the question is Yes, the YES branch should be taken. If the answer is No, the NO branch should be taken and the HEP is 1.0.

Branch Point 2: Information Obviously Incorrect

Definition: This branch point addresses whether the primary information is obviously incorrect or ambiguous, and is only questioned if there are alternative or supplementary means for obtaining relevant information. (This is a question related to the indication itself; the fact that the additional information can reveal that the indication is incorrect is addressed in branch point 3.) For example, if an indicator is blank it is clearly unavailable; this might occur on a loss of a DC power bus. As another example, an indicator being pegged high or low could be understood as being incorrect, particularly if the expectation is that it should be trending rather than steady. Another example is conflicting indications, e.g., two level gauges showing high, a third showing low.

Explanation: The purpose behind including this branch is that if the data is obviously incorrect, the need for consulting additional information sources is enhanced. To determine which direction to take at the branch point for the case of a single indicator the analyst should develop an understanding of such things as whether an instrument fails high or low and is known to fail that way, or whether it fails as is, in which case, it would be much more difficult to detect an incorrect reading. For data that is masked or distorted by additional failures, this is probably not likely to be answered in the affirmative. The reason for asking this question is to make a distinction between the cases where it is clear that the crew should seek additional data and those where it is not.[8]

In addressing this branch point, the following questions may be helpful:

a) Is the indication unavailable or clearly failed?
b) Is the indication ambiguous AND a reason can be postulated why the indication is not accurate? Such ambiguity can occur if, for example, the indication does not directly indicate the operational status, functionality, or integrity (as applicable) of a piece of equipment.
c) Is the instrument known to be unreliable, inadequate or inconsistent under plant conditions similar to those expected in the scenario?
d) Is the system behavior unexpected or unexplained?

➔ If none of these apply, then choose the NO branch. If *any* apply, take the YES branch.

Branch Point 3: Guidance to Seek Confirmatory Data

Definition: This branch is related to whether there is guidance that would lead the crew to consult the alternate sources of data and the nature of that guidance. This guidance should include both guidance on the need to consult alternate sources of data and guidance on where

[8] For cases where the information is gained from multiple indicators, it is anticipated that this would be considered when the PRA scenario results in conflicting indications, and this will be a unique application of this tree.

to seek confirmatory data (e.g., what other parameters or indications will allow the operators to correctly understand the plant status).

Explanation: Guidance, whether it be in the form of written procedure or instilled by training, will increase the likelihood that the additional data sources are used correctly to determine the plant status. Note that the guidance is not restricted to confirmation of the (incorrect) data but could be related to another aspect of the function being addressed (e.g., confirming level rather than flow). To credit guidance in the form of general training or standard work practices, the training must be related to the type of indication of interest or action being performed (e.g., when checking for flow, always confirm by checking level is changing). This is expected to be the norm for US NPPs, however, there may be indicators which are generally not important enough to emphasize in training, but might become key in a given scenario. In some of these special cases, there may specific training or guidance on the action of interest in the form of callouts or warnings in the procedure that can be credited.

On the YES path of the alternate/supplementary source of information branch, there are two cases, the first corresponds to the case where it is not clear that the data is incorrect (on the NO branch at branch point 2), the second for when it is obviously incorrect (on the YES branch at branch point 2). In the first case, successful recovery will rely more on standard work practices and on the innate knowledge of the crew to resolve conflicting or missing indications. An example of this is a closed recirculation valve may indicate flow when flow is expected (not obviously incorrect), but operators are trained to confirm by examining level. In the second case, where the information is obviously incorrect, such as an unavailable indication, the crew will be strongly motivated to use alternate sources of information and to act upon it with less reluctance than in the first case. While the questions below are the same for both cases, the strength of the compensating evidence will be greater for the second case.

In addressing this branch point, the following questions may be helpful:

a) Is it standard operational practice to confirm or corroborate that the parameter or status of the function/system/component as indicated by the primary source is as indicated, using alternate sources of information?

OR

The procedure in effect leads to obtaining other (correct) information that is correct and would conflict with the incorrect information.

b) In the case of conflicting information, is the latter (confirmatory) information given sufficient credence to result in a correct plant status assessment? In other words, is the new information sufficiently compelling to alter the crew's mental model of the status of the function being addressed by the procedure?
This may be determined by discussing with the crew their training with respect to the indications and scenario being modeled and their understanding of the significance of the alternate information.

➔ If *either* a) or b) is *not* met, take the NO branch. If they are both met, take the YES branch.

Branch Point 4: Distraction

Definition: The concern is whether there is something about the scenario being analyzed that results in distraction such that the likelihood of obtaining the correct information from the alternate sources is lessened.

Explanation: Even though the crew may know they should collect additional data, other factors may lead to the data not being collected and acted on in time. Workload is likely to be a significant factor here. In this context, workload is used to represent the scope and resource requirements of the activities that the crew is expected to be performing concurrently with the

task being addressed in this HFE (W2). Time available may also be a factor in that more time available may allow for a greater chance of innovative thinking, particularly when there is not clear guidance on where to seek confirmatory data.

The following question may be useful to assist the analyst in addressing this branch point:

a) Does the response occur at a time when the responsible operator needs to attend to multiple sources of information, alarms or tasks, or alternatively, while the additional information is not yet sufficient to give a clear indication that the primary indication is incorrect?

➔ If the answer to this question is Yes, take the HIGH branch. Otherwise, take the LOW branch. If there is ample time, such that there is time and manpower available to respond after the existing distractions die down, then the LOW branch can be taken. To answer this question the analyst must have an understanding of where this activity fits in with all the other coincident crew activities. Therefore, the response is driven by the qualitative analysis, and in particular the time line of the events and required responses.

5.2.3 SA-2: Wrong Data Source Attended to

5.2.3.1 Definition of CFM

The crew knows they have to obtain specific information, and the desired information is available, but the crew consults the wrong source. This is intended to capture slips in attending to the data (i.e., the crew has the right intent, but attends to the wrong target).

Note: A second possibility involves the crew formulating the wrong idea of what information is needed (that is, the crew goes to the wrong data source thinking that is the one they are supposed to consult). This is assumed to be covered by the CFM 'misinterpret procedures' or those cases involving an incorrect mental model of the plant status which are captured in the CFMs 'critical data dismissed' and 'premature termination of critical data collection'. Further, failure while executing a plant change that result from consulting wrong data is assumed to be captured in the CFMs associated with failure to execute. The current CFM is associated with plant status assessment.[9]

5.2.3.2 Applicability

The HFE is related to a response for which one of the critical tasks is obtaining a piece of data which is used to determine the correct response. This is applicable to a directed search for data (whether it is directed by procedure or by good practice). In this scenario, the operator knows what data is needed and has decided to collect it. This error may be due to a slip resulting in consulting the wrong data source and could include errors such as looking at the wrong train, going to the incorrect indicator, etc. This CFM does *not* include the misreading of procedures, misperception of the correct data, data misleading or unavailable, or having an incorrect mental model of the plant system (not the plant status per se) since these are each addressed by other CFMs. In contrast to the CFMs 'data misleading or unavailable' and 'data misperceived', this CFM involves the crew consulting a wrong source of data. This particular CFM may be particularly relevant to the study of errors of commission.

[9] In the context of modeling HFEs as errors of omission (failure to perform a required function), it doesn't matter what other data they collect, only that they don't get the right data. To model errors of commission (i.e., an incorrect response with consequences that are different from failing to respond) on the other hand, the analyst would have to identify what data was used to formulate the incorrect response. Therefore, when modeling errors of commission, the search for relevant plant signatures to the second case described above is more constrained.

This CFM is applicable when the following are possible: there is more than one train, several similar indicators are grouped, etc. The failures might result from slips or having an incorrect or poor mental model of the plant system (not the plant status per se but poor familiarity with the layout for example).

5.2.3.3 Development of Decision Tree

This decision tree questions the HSI aspects related to the potential for confusion, the level of workload, the familiarity with the data source, and the potential for recovery.

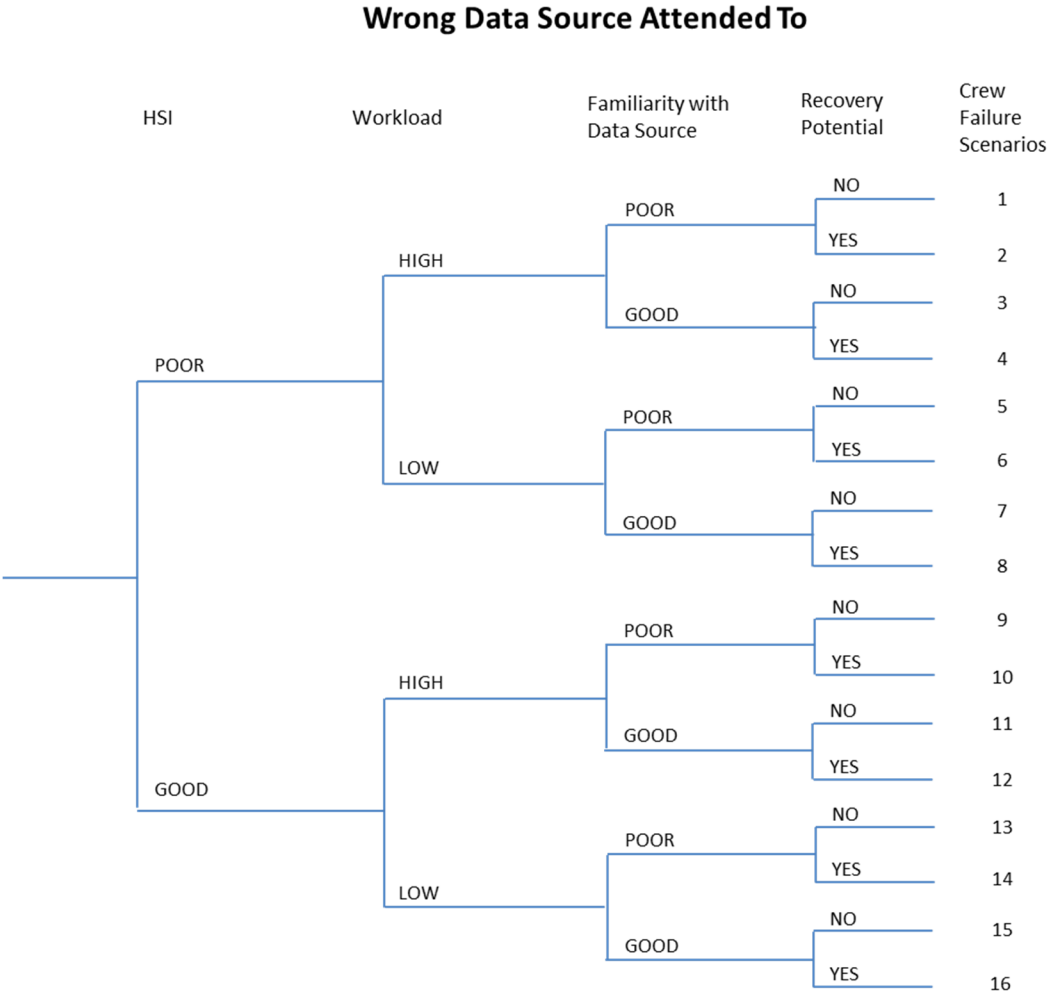


Figure 5-3. Decision Tree for CFM 'Wrong Data Source Attended To'

Branch Point 1: HSI

Definition: For the purposes of this branch, HSI refers to the layout of the indications that provide the data. The purpose of this branch point is to assess whether there is potential for the target source of data to be confused with another that gives the data in a similar format so that it could reasonable be confused with the target.

Explanation: The rationale for assessing this branch point is that the most probable reason for reading the wrong data is that there are other sources that are similar to or in close proximity to the correct data source.

In addressing this branch point, the following questions may be helpful:

a) Is the source of data isolated in a clearly defined location?
b) If the source of data part of a group of collocated sources that are similar in nature, but the labeling (e.g. divisionality) is clear and unambiguous or indicated on schematics?

➔ If the answer to *either* of these is Yes, take the GOOD branch. If No, take the POOR branch

Branch Point 2: Workload

Definition: This branch addresses the cognitive workload. Workload is considered to be an important PIF in that, if it is high enough, it can be a distracting factor which reduces the attention paid to the data collection and therefore increases the likelihood of error.

Explanation: There is always a certain level of cognitive workload, therefore the purpose of this branch is to distinguish between those contexts where the workload is normal in the sense that it is at an anticipated level and within the scenarios experienced by the crew in training and or actual operation. The cognitive workload is considered high when it is outside the expected level. This could arise when the number of tasks that are required to be performed within the same time frame is high, or when tasks have to be performed expeditiously (primarily W2 and W6). In this sense, workload can be considered as a surrogate for time pressure.

In addressing this branch point, the following questions may be helpful:

a) Is the crew member responsible for obtaining the data also responsible for other coincidental tasks?
b) Is the task complex (in the sense of requiring a number of different activities within a relatively short time)?

➔ If *either* of these is true, take the HIGH branch. Otherwise, take the LOW branch.

Branch Point 3: Familiarity with the Data Source

Definition: Familiarity with the data source addresses the level of training and experience the crew has with this specific data source.

Explanation: The purpose of this branch is to determine whether the training and the experience of the crew make it unlikely that the wrong source would be attended to. Training can be a compensatory factor for a poor HSI, on the contrary, even when the HSI is well designed, the crew could make an error if they have never or rarely been exposed to this data source.

In addressing this branch point, the following questions may be helpful:

a) Is the crew well trained on this source of information?
b) Does the training emphasize the train/segment separation?

➔ If the answer to *both* of these is Yes, take the GOOD branch. Otherwise, take the POOR branch.

Branch Point 4: Recovery Potential

Definition: This branch addresses the likelihood that given an incorrect plant status assessment has been formed as a result of consulting the wrong data source, the subsequent actions of the crew allow for a realization that an error has been made and the procedures and or training lead the crew to correct their error in time to prevent failure of the function captured by the HFE.

Explanation: The CRD should have identified a potential recovery path, and this branch assesses whether that recovery can be credited for this specific HFE. The following is additional guidance specific to this CFM. This error is modeled as being driven by slips rather than a cognitive misunderstanding. Therefore, it is considered to be relatively easily recovered

For recovery that occurs once the crew has committed to an (unknown to them) incorrect response, the analyst needs to postulate what response the crew is taking as a result of the wrong data. Then, the opportunities for the crew to realize that the response was not as anticipated and the practices that would lead them to question the original data would need to be evaluated. For example, the analyst should determine whether and how the crew is monitoring the status of the plant to see if the plant response is as expected (e.g., if they think they are adding inventory in all likelihood a RO will be checking level and will recognize that it is not being restored as expected).

NOTE: Credit for self-recovery or immediate recovery by another crew member (peer-check) is already accounted for in the base HEP; this recovery is a new cue or indication that will lead the crew back to a success path. This makes sense because there will almost always be some oversight, or more than one person involved in a response. This is particularly true for those cases where there is no time pressure.

5.2.4 SA-3: Critical Data Misperceived

5.2.4.1 Definition of CFM

A critical piece of information that is required to develop a plant status assessment is misperceived. A critical piece of data is one that, when misperceived in a certain way will lead to an incorrect response in that it leads to taking an incorrect or inappropriate path through the procedures or executing a response incorrectly.

5.2.4.2 Applicability

This CFM is intended to cover things such as mistakes in reading the values of parameters from a display or mistakes in determining the equipment status from indications on the control panel. This CFM is applicable to a scenario for which one of the contributing critical tasks is using the datum directly as a discriminating factor related to a decision. In applying this CFM, the HRA analyst will have performed the task analysis and identified what incorrect value/status can lead to failure. Examples include: mistaking on for off, shut for open; value as X rather than Y. For the latter, typically this value will be compared to a benchmark, such as “Is RCS pressure greater (less) than Y psia”, “WR SG level at or below X%”, or “suppression pool temperature at or below 110°F”. In this case, the extent of the error necessary to cause failure is defined. Another case might be “Is the parameter within the bounds X to Y”. Again this will define the extent of the error needed to cause failure. This CFM is intended to be a “local” failure at the level of the specific item of data.

Misperception of trends is covered in other CFMs, e.g., not monitoring with appropriate frequency, or data misleading (if the cause is a result of say a partial failure).

5.2.4.3 Development of Decision Tree

The reasons why an operating crew might fail include difficulties with the source of the data, which include limits on the source’s discriminating power and its accessibility, exacerbated by a lack of familiarity of the data source and any potential biases related to expectations on what the value of the data usually is or “always has been”. A high workload is postulated to increase the likelihood of incorrect processing by limiting the time available to ensure the correct assessment is made. Furthermore, the environment in which the data is to be collected may also have an adverse effect.

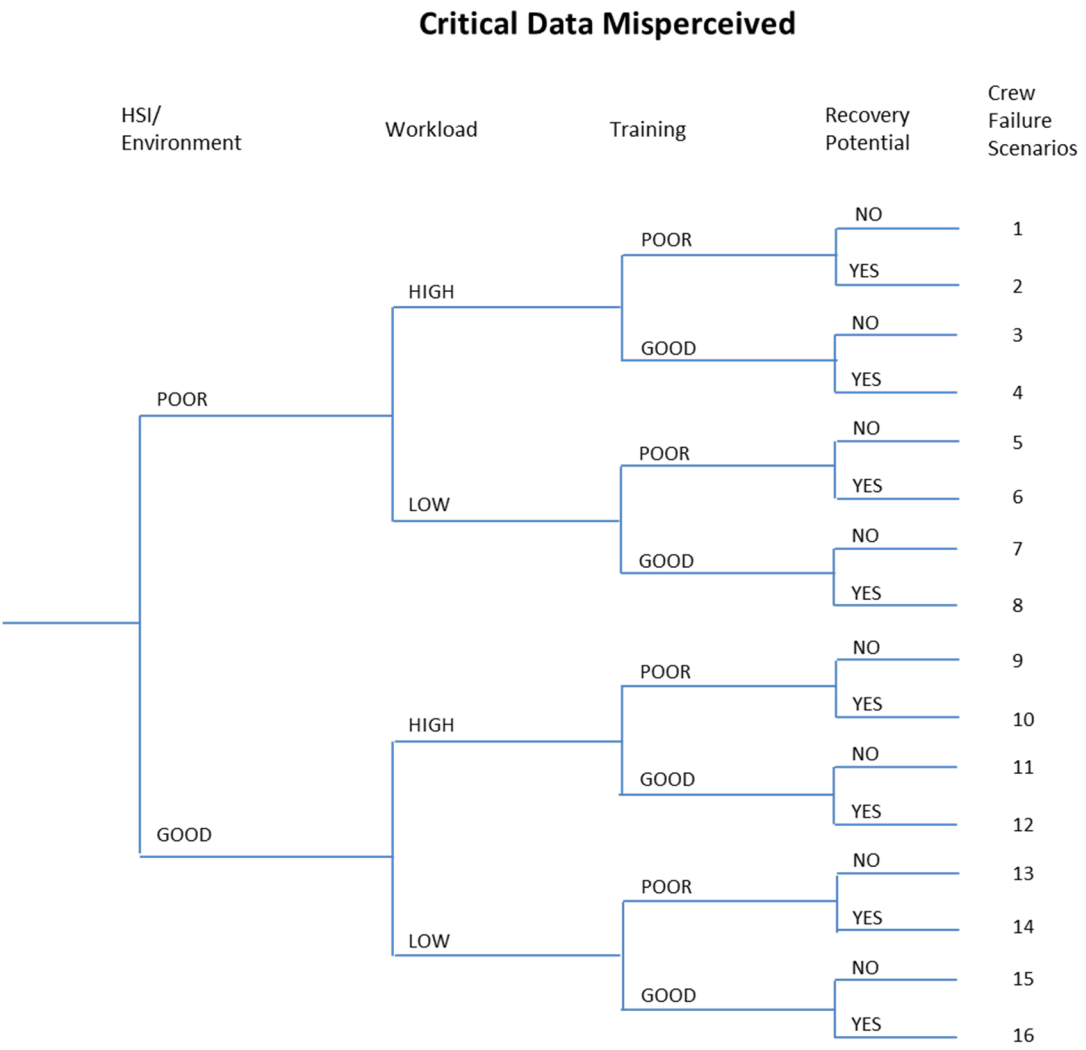


Figure 5-4. Decision Tree for CFM 'Critical Data Misperceived'

Branch Point 1: HSI/Environment

Definition: The aspects of HSI and environment that are relevant here include the nature of the indicator and its location and environment, given the operator is looking at the correct data source.

Explanation: The issue addressed by this branch point is whether the information source can be difficult to interpret for the subject scenario. This needs to be tailored to the type of information source, so there could be different issues depending on the nature and location of the source (e.g., in control room or local ex-control room) and conditions, and whether the instrument is discriminating enough for the requirement (typically it will be). For the GOOD branch, the information source is well engineered from an HSI standpoint, and there are no detrimental environmental factors, so that there is little chance for ambiguity with respect to its meaning and therefore a very small chance of misinterpretation. The POOR branch would correspond to the situation where there are potential difficulties arising from scenario specific environmental factors, or a poor HSI. The following examples represent how the HSI may impact the salience of the cues:

a) If the cue is not presented to the operator with sufficient strength/energy to distinguish itself from existing background noise such that it activates a sensory response in the operator, the operator may misperceive it.
b) If the cue is presented in such a way that it is difficult for the operator to change/move their focus of attention to it, the cue may be misperceived.
c) Operators may misperceive cues from cluttered displays that are not salient enough.
d) The quality and amount of information provided in the cue has an effect on whether the cue will be accurately detected. Specifically, the more complex the cue, the less likely operators are to correctly recognize specific parts of the cue.
e) Verbal (word) salience can affect proper perception.
f) Back panel is not bad HSI if you choose to go back there the readability is fine whereas, in another CFM, that would be considered bad HSI based on location and if in the field of view.

In addressing this branch point, the following questions may be helpful:

a) Are the indications clear and unambiguous?
b) Is the information easy to read?
c) Is the range (or band) with which the information is to be compared clearly identified on the display?
d) Is the environment in the location of the indicator/source of information nominal (i.e., not challenging due to noise, heat, humidity, etc.)?
e) Are the indicators/sources of data easy to locate and read?

➔ If the answer to *any* of these questions is No, take the POOR branch. Otherwise, take the GOOD branch.

Branch Point 2: Workload

Definition: Workload in this context refers to cognitive workload.

Explanation: Workload is treated here as a surrogate for distraction, which could lead to taking less care when reading the datum. When workload is high there is an increased chance of incorrectly processing information. Workload in this context refers to the number and/or nature of the activities that the person responsible for collecting the data is performing at the time the data is to be collected (primarily W2 and W6). The nature of the other activities comes into play if they are given a higher priority than the task. However, this CFM is addressed contingent upon the operators having determined that they need this data, so at that point in time the conflicting activities do not directly play a role. However, they may lead to time pressure, or hurrying the operator to get the data. Furthermore, many slips of this nature are likely to be caught by another crew member, particularly when the data is communicated to another crew member who may question the data if it seems incorrect. Time pressure will have a negative impact on this potential for immediate recovery. The LOW Workload branch corresponds to there being no interference from other tasks. The HIGH Workload branch corresponds to a scenario where there are several activities on-going that are of equal or higher priority.

In addressing this branch point, the following questions may be helpful:

a) Does the need to obtain information occur at a time when the operators are still in the process of determining the plant status?
b) Does this occur at a time when there are several alarms or indications or tasks that need attention?
c) Is the scenario one for which the number of tasks the crew has to perform in the time available higher than would be typically addressed in training?

➔ If *any* of these is true, take the HIGH branch. Otherwise, take the LOW branch.

Branch Point 3: Training

Definition: The aspects of training that are relevant to this branch are those that are specific to either the scenario or the specific indicator.

Explanation: Training is a compensatory factor if it is geared to scenario specifics where the information source may be problematic or cognitive workload is relatively high. The compensatory factors will be different depending on the path so far. Training as a compensatory factor is most relevant for those situations where there could be some ambiguity with respect to the meaning of the datum. This does not refer to the general training related to reading displays, which is assumed to be optimal for all crews. This is likely to be most relevant for either a poor HSI or a high workload situation. The GOOD Training branch would be taken if it is clear that the response for which this data collection is critical is given a higher priority than other actions, or if special training is given to interpreting the data should there be potential ambiguities. The POOR Training branch would be taken if there is no specific training provided, i.e., no compensatory factors can be identified.

In addressing this branch point, the following questions may be helpful:

a) Has the crew been properly trained to understand and deal with scenarios in which the information source may provide difficulties?
b) Is the significance of the decision that is based on obtaining this information correctly given a high priority compared to other concurrent tasks?

➔ If the answer to *both* is No, take the POOR branch. If Yes to either, take the GOOD branch.

Branch Point 4: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.15. The following is additional guidance specific to this CFM.

Definition: This branch addresses the possibility that given an incorrect plant status assessment has been formed as a result of misperceiving data, and an incorrect path through the procedures or an incorrect execution path has been chosen, subsequent actions of the crew allow for a realization that an error has been made and the procedures and or training lead the crew to correct their error in time to prevent failure of the function captured by the HFE.

Explanation: When applying this CFM to a CRD branch, the data that is misperceived will have been identified as being that which causes the failure of the task represented by the branch, whether that task is a decision, a transition to another procedure, or initiating a response. The data being misperceived results in an incorrect plant status assessment, and therefore recovery would most likely take place after the response has been initiated. For failures in the plant status assessment or response planning, the CRD will include potential opportunities for recovery. To take any credit for recovery, the analyst must develop an understanding of what happens to the plant given that the response taken is consistent with the misperception of the data and what the crew will be doing subsequent to the error. They may be following an incorrect path through the procedures or they may have failed to initiate, terminate or control a system.

NOTE: Credit for self-recovery or immediate recovery by another crew member is already accounted for in the base HEP; this recovery is related to a new cue or indication that will lead the crew back to a success path. There will almost always be some oversight, or more than one person involved in a response. This is particularly true for those cases where there is no time pressure.

For recovery that occurs once the crew has committed to an (unknown to them) incorrect response, the analyst needs to postulate what response the crew is taking as a result of the misperceived data. Then, the opportunities for the crew to realize that the response was not as anticipated and the practices that would lead them to question the original data would need to be evaluated. For example, the analyst should determine whether and how the crew is

monitoring the status of the plant to see if the plant response is as expected (e.g., if they think they are adding inventory in all likelihood a RO will be checking level and will recognize that it is not being restored as expected). This should be captured in the CRT. The analyst needs to account for the context, including ensuring there is sufficient manpower and time, before deciding whether credit can be given for recovery.

5.2.5 SA-4: Critical Data Dismissed/Discounted

5.2.5.1 Definition of CFM

The crew is aware of and has obtained the correct information (e.g., the value of a key plant parameter, the status of a piece of equipment, information that has been communicated by another person, etc.), but has discounted it from the assessment of the plant status (and, therefore, represents an incorrect synthesis of the information they have).

5.2.5.2 Applicability

The PRA scenario is one in which a successful response involves the crew obtaining a critical piece of data in order to formulate the correct plant status assessment and therefore take the appropriate response. An example of such a piece of data is the rising level in the sump to indicate or confirm a LOCA. This CFM is applicable when the information being dismissed is an essential part of assessing the plant status for which there is one (or possibly more than one) successful response. This particular CFM represents a deliberate discounting as opposed to “I’ll get to it later”, or not obtaining the data because of misinterpreting or skipping a step in the procedure. Since the cognitive process of establishing a mental model is likely to be iterative and cyclic in nature, this CFM is applicable when an assessment of plant status that is made on partial information leads to a failure. This possibility is questioned in the decision tree. Determining whether this CFM is relevant requires an understanding of the chronology of the way information is received or obtained to develop an assessment of the plant status.

5.2.5.3 Development of the Decision Tree

Generally a crew or operator may dismiss or discount critical data because of a bias in their training or knowledge/experience/expertise such that they develop an inaccurate plant status assessment. In addition, poor procedural quality or poor HSI output could exacerbate the incorrect assessment.

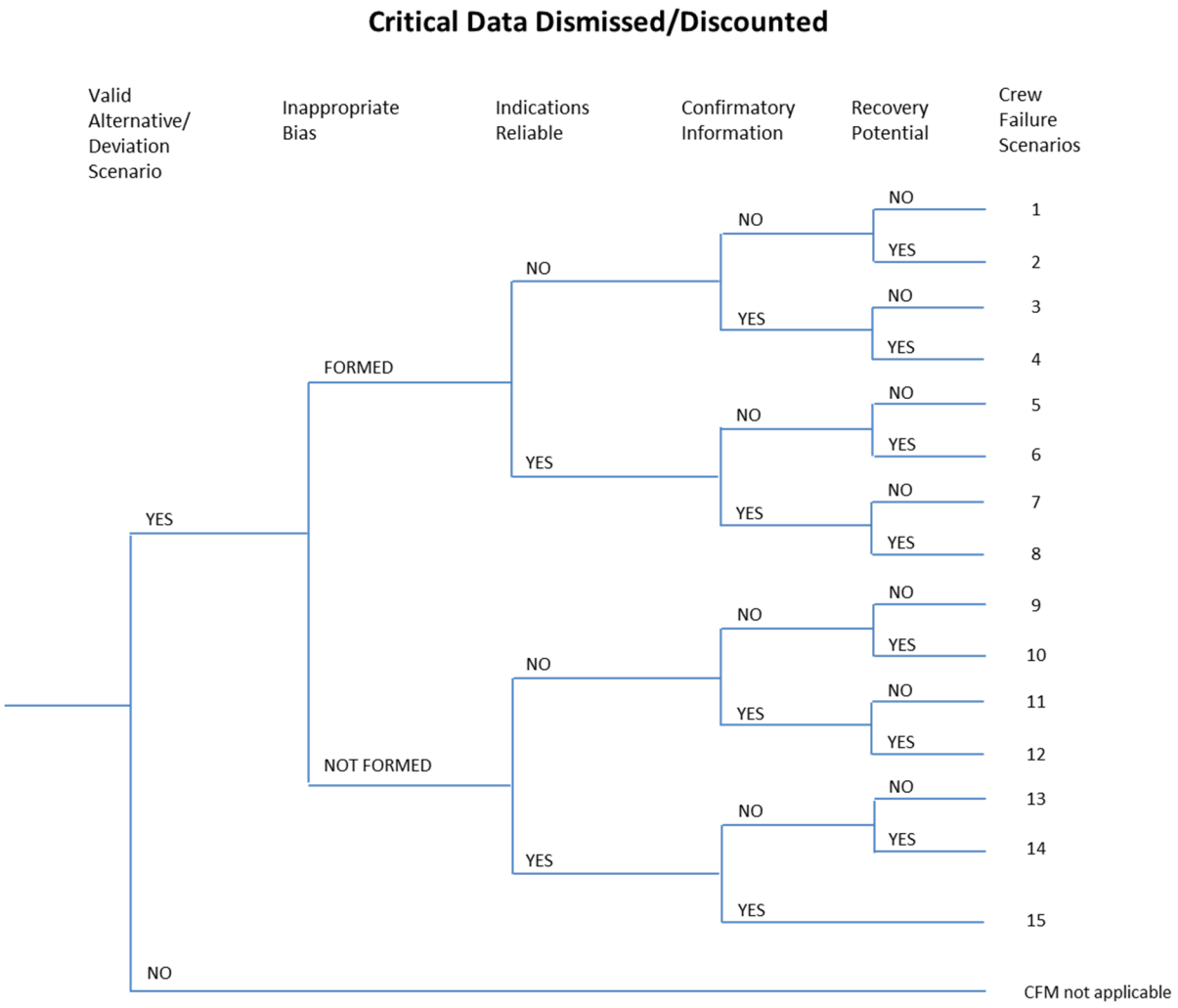


Figure 5-5. Decision Tree for CFM 'Critical Data Dismissed/Discounted'

Branch Point 1: Valid Alternative/Deviation Scenario

[*NOTE: This branch point is not intended to be a reflection of the crew's biases, but is intended as a screening question to identify those scenarios when an incomplete data set provides a viable plant status, i.e., one that the crew could believe was correct based on their experience and training. In other words, the signature presented by the incomplete data set is consistent with that of a potential plant state.]

Definition: The first branch assesses whether, in the absence of the critical data that is the subject of this CFM, but with all the data pertaining to the plant status taken into account, there is a plant status that is valid and within the spectrum of plant conditions that is encompassed by knowledge base of the crew.

Explanation: This CFM is only considered to be relevant if there is a valid reason why the crew would dismiss a piece of data, and this might occur if there were sufficient similarity between the signature of the real plant scenario (as given by the set of plant parameters, including equipment status indications) and another whose signature is given by the same set of indications minus the critical piece that is dismissed.

To address this branch point, the analyst should answer the following:

a) Is there a plant signature that, with the collection of the critical information dismissed, is an anticipated plant state? To answer this question it is helpful to have a map of the plant state parameters associated with the scenario and an understanding of what the procedures instruct the operators to do both with the information included and omitted.

➔ If there is such a scenario, take the YES branch. If such a valid scenario does not exist, this CFM is not applicable.

Note: This is not likely to be the case for the major classes of accidents (e.g., LOCA, SGTR) since they have very distinct signatures, but may occur as a result of equipment failures that change the nature of an accident in a subtle way. Identifying these subtly different accident scenarios is challenging since it requires a detailed understanding of the effect of equipment failures on the parameters the crew would use to determine the plant status.

Branch Point 2: Inappropriate Bias

Definition: Given that there are possible alternative scenarios that have similar, though not identical signatures, this branch point addresses whether a bias from training and knowledge/experience/expertise with respect to the plant status could affect the crew's behavior.

Explanation: Even if there are similar signatures, the likelihood of the critical data being dismissed will be enhanced if there is a strong bias towards the incorrect signature based on training and experience. The questions to be asked are whether the training and experience are sufficient to create a strong expectation that the critical data (i.e., that which is necessary to make the correct distinction between the correct and the alternate plant status) can be dismissed.

In addressing this branch point, the following questions may be helpful:

a) Is training on the *correct* scenario more frequent that that of the *incorrect* scenario?
AND

b) Is the crew familiar with the data source and what it implies for the plant status independent of the specific scenario?

➔ If the answer to both (a) and (b) is Yes, then use the NOT FORMED branch. Otherwise follow the FORMED path. The assumption here is that this type of error is likely to happen only if the crew has little or no actual experience with the scenario (which is probably true of most PRA scenarios). Hence the focus on training rather than experience.

Branch Point 3: Indications Reliable

Definition: This branch point assesses the crew's perception of the reliability of the information that is being dismissed. This is another form of crew bias.

Explanation: If the crew judges the plant indications (HSI output, procedural quality, etc.) to be unreliable, this is an additional reason why they may be likely to dismiss the information that the indicators are providing. This does not apply when the known areas of unreliability are well understood by the crew or when a warning of the potential unreliability is given in the procedure.

Note: This question is not asking about the reliability of the data in this scenario specifically; by definition, in this scenario the indications are indicating the correct status (incorrect or misleading indicators are dealt with in another CFM). This branch point is asking about the operator's *perception* of the reliability of that indicator.

An example might be a crew that becomes accustomed to discounting the flow indicator in on valve because the valve is known to be leaky and indicate flow when the valve is closed. In this case, the indicator would be indicating correctly (showing flow because the valve is open), but

the crew will discount the data. There is potential to confirm the data (i.e., the rate of flow is much higher when the valve is actually open v. leaking), but to credit this, the operators would need to be accustomed – either through training or directed by the procedures – to confirming the data; this is addressed in the next branch. This sort of failure was seen in the TMI accident.

In addressing this branch point, the following questions may be helpful:

a) Is the indication potentially ambiguous AND a reason can be postulated why the indication is not accurate? Such ambiguity can occur if, for example, the indication does not directly indicate the operational status, functionality, or integrity (as applicable) of a piece of equipment.
b) Is the instrument known to be historically unreliable, inadequate or inconsistent?
c) Is there something about the specific plant/environmental conditions expected in the scenario (i.e., excessive heat or pressure) that would cause the operators to question the reliability of that indicator given the scenario?

➔ If *any* of these applies, then choose the NO branch. Otherwise, take the YES branch.

Branch Point 4: Confirmatory Information

Definition: This branch addresses whether, before dismissing any piece of information, the practice of the crew, whether by procedure or standard good practice, is to search for confirmatory information, that if obtained would likely result in the information not being dismissed. This guidance should include both guidance on the need to consult alternate sources of data and guidance on where to seek confirmatory data (e.g., what other parameters or indications will allow the operators to correctly understand the plant status).

Explanation: If it is the case that, before dismissing any piece of information, the crew searches for some confirmatory information, this should lessen the likelihood of discounting the information. There may be specific procedural steps that the operators engage in to confirm the information and/or the operators may perform confirmatory checks as a matter of good practice. To credit guidance in the form of general training or standard work practices, the training must be related to the type of indication of interest or action being performed (e.g., when checking for flow, always confirm by checking level is changing). This is expected to be the norm for US NPPs, however, there may be indicators which are generally not important enough to emphasize in training, but might become key in a given scenario. In some of these special cases, there may specific training or guidance on the action of interest in the form of callouts or warnings in the procedure that can be credited.

In addressing this branch point, the following questions may be helpful:

a) Are there additional indications that would typically be used to confirm the plant status indicated by the information (e.g., pump amps to confirm a pump is running correctly or not)?
b) Is checking these additional sources emphasized in training and considered standard plant practice?

➔ If the answer is Yes to *both* these questions, take the YES branch. Otherwise, take the NO branch.

Branch Point 5: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.15. The following is additional guidance specific to this CFM.

Definition: This branch addresses the likelihood that given an incorrect plant status assessment has been formed as a result of consulting the wrong data source, the subsequent actions of the

crew allow for a realization that an error has been made and the procedures and or training lead the crew to correct their error in time to prevent failure of the function captured by the HFE.

Explanation: The CRD should have identified a potential recovery path, and this branch assesses whether that recovery can be credited for this specific HFE. This branch addresses the possibility that, even if the crew/operator makes the wrong decision initially, there is a means of timely self-recovery. For instance, the operator (given the incorrect plant status assessment) might be expecting a particular plant response. If this response does not occur or is different than what is expected, the operator may re-analyze the plant status which may result in correcting the previously inaccurate assessment. In addition, future procedural steps may lead the operators to make the appropriate decisions to get back on track for that function. If the crew has opportunities to reassess the plant status, this could serve as a recovery potential.

For this failure mode, the recovery cue must be strong enough to force the operators to reassess their mental model. This might include, for instance, procedure-directed collection of new data from a reliable data source, or intervention by the TSC.

5.2.6 SA-5: Premature Termination of Critical Data Collection

5.2.6.1 Definition of CFM

The crew stops collecting data too early and assesses the plant status on an incomplete data set, with the understanding that if they had continued to collect data they would have come to a different plant status assessment.

5.2.6.2 Applicability

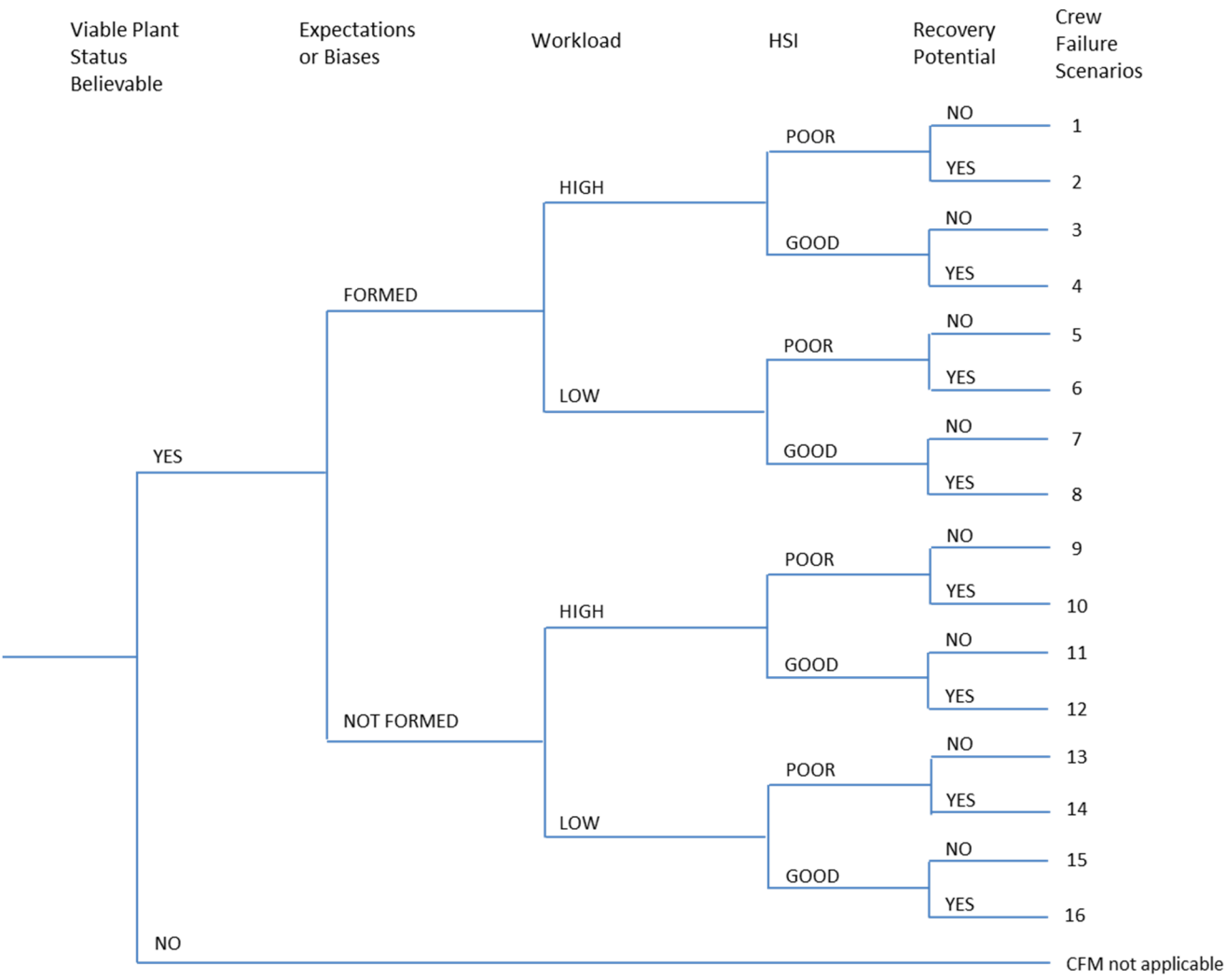
The PRA scenario is one in which success requires the crew to assess the plant status correctly. This is done by collecting sufficient information to validate the plant status. This CFM is applicable to the task of collecting the data that is necessary to give an accurate picture of the plant status. Failure will occur if the crew has determined that additional data is not needed because they have decided that they have a sufficient assessment of the plant status to go ahead. In other words, they are confident in their plant status assessment. Since the data being collected is supposed to be germane to the plant status assessment, this CFM is related to the development of the mental model of the plant status. It can be applied to cases where the decision is made based on observing a trend. Specifically, this CFM would apply in the sense that the data collection needed to establish the true trend is prematurely stopped based on an assessment of plant status that fits an existing, incorrect mental model. This CFM does not necessarily imply that the crew has disregarded procedural direction or that they have skipped some procedural steps. For example, it might be the case that the crew is directed to check a system or component status and they feel that due to prior knowledge (e.g., some prior check) they have enough information to answer the question.

5.2.6.3 Development of Decision Tree

The decision tree is developed on the premise that the crew might stop collecting critical data only if they have a tendency to believe that they have a plant assessment that is viable and consistent with the partial plant status signature obtained to that point in time. The viability of the plant status is questioned in the first branch. Not only does the plant status represented by the partial information have to be viable, it also has to be credible to the operators. So, a prerequisite for this CFM to be a contributor to an HFE is that there is a plant status signature

that, with the partial critical information, represents an anticipated plant status.[10] The second branch point determines what the expectations are of the crew and whether they have formed expectations leading them to accept the incorrect plant status represented by the partial information. The crew's development of the plant status assessment can be thought of as a Bayesian process - as new evidence comes in as the crew follows the steps in the procedure, it can change their perception of what's happening to the plant. So this expectation is related to how strongly they believe they already know what's wrong and how likely they are to stop collecting additional data and act on what they know. Training or experience may bias the operator in this direction and is assessed in this DT. Additional factors impacting this CFM are workload, quality of HSI and the potential for recovery.

Premature Termination Of Critical Data Collection



[10] The term anticipated is used in the same sense as in anticipated transient; it is a recognized plant status for which contingencies (procedural guidance) are in place, but it doesn't signify that it is expected with high frequency, merely that it's been thought of and in this case contingencies are in place to deal with it.

Figure 5-6. Decision Tree for CFM 'Premature Termination of Critical Data Collection'

Branch Point 1: Viable Alternative Plant Status Believable

[*NOTE: This branch point is not intended to be a reflection of the crew's biases, but is intended as a screening question to identify those scenarios when an incomplete data set provides a viable plant status, i.e., one that the crew could believe was correct based on their experience and training. In other words, the signature presented by the incomplete data set is consistent with that of a potential plant state.]

Definition: The first branch is intended to assess whether, in the absence of the critical data that is the subject of this CFM, but with all the other data pertaining to the plant status taken into account, there is a plant status that is valid and within the spectrum of plant conditions that is encompassed by the knowledge base of the crew.

Explanation: This CFM is only considered to be relevant if there is a valid reason why the crew would not continue to obtain a piece of data. This can only occur if there was sufficient similarity between the signature of the real plant scenario (as given by the complete set of plant parameters, including equipment status indicators) and another whose signature is given by the same set of indications minus the critical piece that has not been obtained.

To address this branch point, the analyst should answer the following:

a) Is there a plant signature that, with the collection of the critical information terminated prematurely, is an anticipated plant state? To answer this question it is helpful to have a map of the plant state parameters associated with the scenario and an understanding of what the procedures instruct the operators to do both with the information included and omitted.

➔ If there is such a scenario, take the YES branch. If such a valid scenario does not exist, this CFM is not applicable.
NOTE: The search for such scenarios may be challenging, since they are likely to result from subtle changes that may not be captured in typical PRA scenarios, e.g., they may require the existence of partial failures. This CFM may not be invoked frequently.

Branch Point 2: Expectations or Biases

Definition: Given that there are possible alternative scenarios that have similar, though not identical signatures, this branch point is intended to address whether a bias from training and knowledge/experience/expertise with respect to the plant status could result in the crew forming a mental model of the plant status prematurely.

Explanation: Given that there are scenarios with similar signatures, the likelihood that the critical data may not be obtained will be enhanced if there is a strong bias towards believing that the data obtained up to a certain point in time is sufficient to determine the plant status. In other words, this branch is concerned with assessing whether the information to the point where the data collection is stopped is sufficient to form and support a viable mental model. The questions to be asked are whether the training and experience are sufficient to create a strong expectation that the critical data, i.e., that which is necessary to make the correct distinction between the correct and the alternate plant status, is already understood or needs to be obtained.

The assessment of this branch point is somewhat more subjective than that of many other branch points, and it is especially important to understand how the crew is trained and what their expectations are.

The following questions are provided to assist the analyst in addressing this branch point:

a) Is training on the *correct* scenario sufficiently more frequent that that of the *incorrect* scenario that the incorrect scenario is not the expected scenario?

AND

b) Does the crew NOT have a preconceived notion of the parameter value (e.g., from a previous status check accompanied by an assumption that there is not trending)?

➔ If the answer to both (a) and (b) is Yes, then the NOT FORMED branch would be appropriate; otherwise the FORMED path may be chosen. The assumption here is that this type of error is likely to happen only if the crew has little or no actual experience with the scenario (which is probably true of most PRA scenarios).

➔ If there is no or limited training/plant experience with either scenario, and the crew is not especially trained to understand the significance of the subject parameter value in determining the plant parameter, a conservative choice would be to choose the FORMED branch.

Branch Point 3: Workload

Definition: For the purposes of this branch, workload is defined as the cognitive workload at the time this response is being carried out. This could, for example, be high as a result of a number of functions requiring attention during the same time frame.

Explanation: In this branch point, workload is seen as a balance between available time, number of simultaneous tasks and available manpower (including W2, W3 and W6). High workload, particularly if it induces a sense of urgency (i.e. the crew recognizes this response has to be dealt with quickly), can have a negative effect on performance and enhance the likelihood that the data collection is prematurely terminated. High workload may be defined as the need to address multiple tasks which could be cognitively taxing and/or allow the operator to become distracted away or redirected from the task at hand. High workload may also be a function of the complexity of the tasks and the need to complete them in a time-dependent situation in which time is limited.

In addressing this branch point, the following questions may be helpful:

a) Does the need for this response occur when other high-priority tasks or procedures are being employed (or the crew needs to respond to several tasks)?
b) Is the accident scenario such that the crew may be interrupted in the middle of their task to attend to another task or person?
c) Does this occur when there is a problem or issue that arises that needs to be resolved immediately? Alternatively, is this task one that might be seen as not needing to be attended to immediately such that another pressing task may take precedence and distract the crew away from the original task?
d) Are the tasks at hand complex and need to be accomplished in a limited amount of time?

➔ If any of these are true, the HIGH branch should be taken. Otherwise, the LOW branch should be taken.

Branch Point 4: HSI

Definition: For the purposes of this branch, HSI refers to the clarity and ease of access to the indications that provide the data.

Explanation: If the data is difficult to obtain, it is more likely that termination of its collection will be made prematurely.

The following question should be answered by the analyst in addressing this branch point:

a) Is the data/information given by the HSI available, prominent, distinctive and unambiguous?

➔ If the answer to the question is No, the POOR branch should be taken. Otherwise, the GOOD branch should be taken.

Branch Point 5: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.15. The following is additional guidance specific to this CFM.

Definition: This branch addresses the likelihood that given an incorrect plant status assessment has been formed as a result of not collecting all the relevant data, the subsequent actions of the crew allow for a realization that an error has been made and the procedures and or training lead the crew to correct their error in time to prevent failure of the function captured by the HFE.

Explanation: The CRD should have identified a potential recovery path, and this branch assesses whether that recovery can be credited for this specific HFE. The following is additional guidance specific to this CFM.

This branch addresses the possibility that, even if the crew/operator makes the wrong decision initially, there is a means of timely self-recovery. For instance, the operator (given the incorrect plant status assessment) might be expecting a particular plant response. If this response does not occur or is different than what is expected, the operator may re-analyze the plant status which may result in correcting the previously inaccurate assessment. For example, if there is time and it is standard practice for the plant to do a crew brief in the form of "in the next 10 minutes we should expect the plant to do X (given diagnosis Y)" and X never happens, then that would be a cue to reexamine their mental model. In addition, future procedural steps may lead the operators to make the appropriate decisions to get back on track for that function. If the crew has opportunities to reassess the plant status, this could serve as a recovery potential. The cue has to both provide the needed information and be strong enough to for the crew to reassess their mental model.

To take any credit for recovery, the analyst must develop an understanding of what happens to the plant given that the response taken is consistent with the crew's plant status assessment with the data collection terminated prematurely and what the crew is doing in terms of where they are in the procedures. They may be following an incorrect path through the procedures or they may have failed to initiate, terminate or control a system. The analyst should determine whether and how the crew is monitoring the status of the plant to see if the plant response is as expected (e.g., if they think they are adding inventory in all likelihood a RO will be checking level and will recognize that it is not being restored as expected). Given that the crew is monitoring the function to ascertain the response is as expected, is there a reason why the original plant status assessment would be challenged and changed?

5.2.7 RP-1: Misinterpret Procedure

5.2.7.1 Definition of CFM

A procedure is misinterpreted in such a way that an incorrect path through the procedures is followed or an incorrect response is initiated.

5.2.7.2 Applicability

This CFM applies to the critical procedure step(s), as identified in the CRD development, which relate(s) to making a decision as to the direction taken in the procedures or in choosing the response needed. Failures that arise from this CFM can result in an inaccurate mental model of the plant status. Misinterpretation is most likely to occur when the procedure is written ambiguously or its structure includes complicated logic. Therefore, this CFM focuses on problems originating with the nature of the procedures. It may be the case that the logic of the procedure is so complicated or convoluted that the appropriate step(s) is buried deep in the

procedure and the crew is not able to get to the appropriate step(s) in time. This case, however, should have been judged as being infeasible and screened from further consideration during qualitative analysis of the HFE.

NOTE: Since the procedures are involved at all stages of the response as we have defined them, namely: plant status assessment; response planning; and execution, this CFM could also apply to phases other than response planning, which is what this CFM was originally intended for. A difficulty with the procedure in the execution phase is best handled in the execution trees (for complex or control cases). However, ambiguity that causes the crew to obtain incorrect information and therefore results in an incorrect plant status assessment could also be addressed by this tree.

This is intended to be applied when the procedure is applicable and correct, but prone to misinterpretation. It is not intended for application when the procedure does not match the plant status. If, when constructing the CRD, it cannot be determined that the procedure provides a correct response, the HEP will be 1.

5.2.7.3 Development of Decision Tree

The starting point for the development of the decision tree is to identify those attributes of the procedure that provide the potential for it to be misinterpreted. Examples include complicated logic or language that is not self-explanatory and is potentially ambiguous. Training and experience in the specific challenging aspects are positive factors that reduce the potential for error. A high workload, however, is a negative factor.

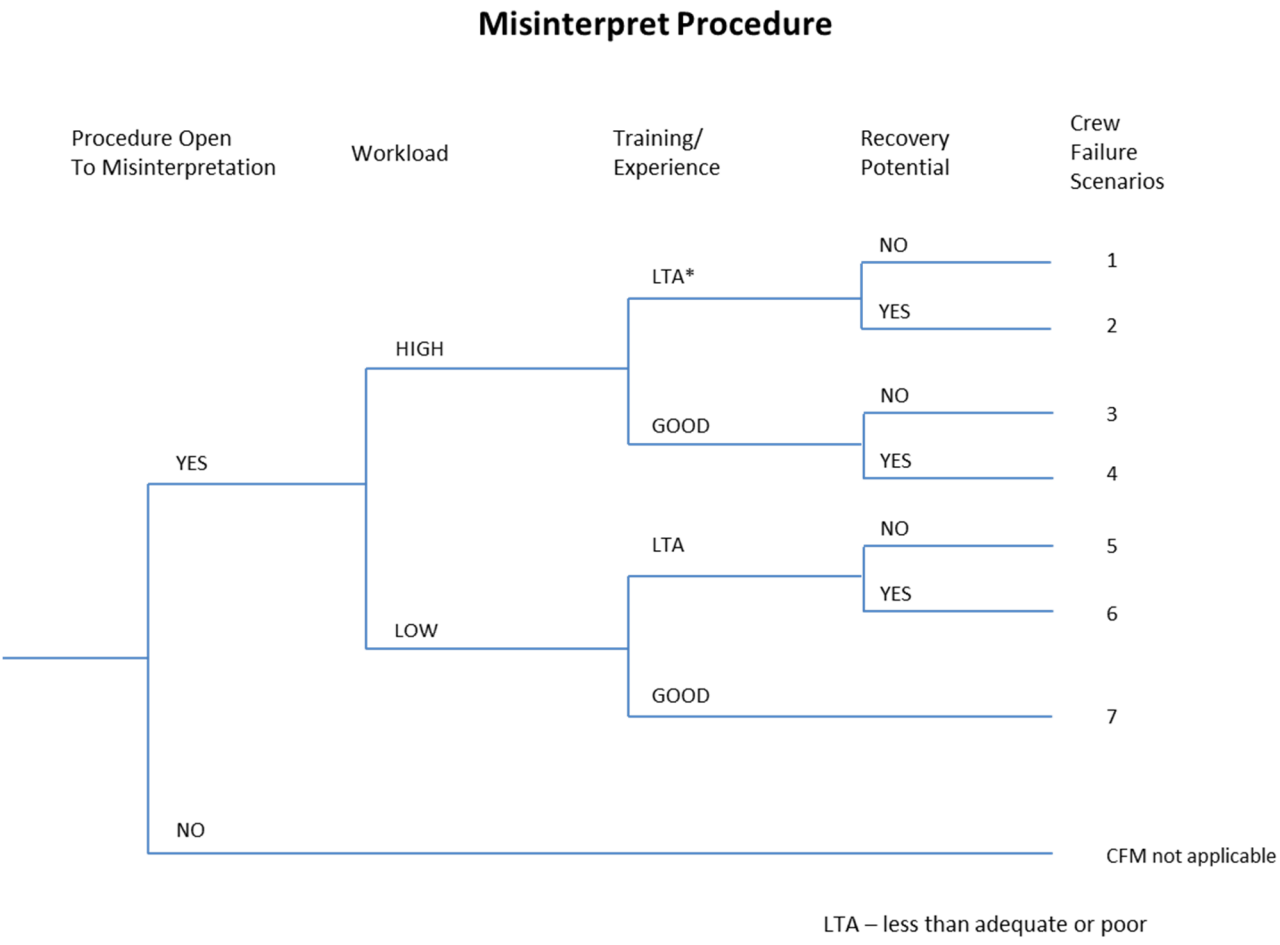


Figure 5-7. Decision Tree for CFM 'Misinterpret Procedure'

Branch Point 1: Procedure Open to Misinterpretation

Definition: This is a screening question and can apply to a single step or group of steps such that if it is misinterpreted it will put the operators on a failure path (e.g., failure to enter the right procedure or branching to the wrong procedure).

Explanation: If the procedures may be easily misinterpreted, for example, they are written poorly, are overly complex, require calculation or non-standard comparison (e.g., is the ratio > 1.5) or have ambiguous wording, they may be easily misinterpreted. If the steps are not clear or lack details for the desired action in the context of the sequence of interest, then the procedure is ambiguous. A procedure may also be judged as being ambiguous if acceptance criteria and tolerances or specific control positions and indicator value are not properly specified (e.g., need to determine the meaning of 'adequate' in the statement "determine if flow is adequate"). A procedure may also be misinterpreted due to charts, graphs or figures that are difficult to read or understand or if the language contains double-negatives. Finally, the complexity of the procedures may be overwhelming if the operator is required to perform calculations or make other manual adjustments without the aid of worksheets.

This CFM is less likely for EOPs, which are well written and vetted, and may be seen more frequently when a critical step comes from an off-normal procedure, alarm response procedure or event response procedure (e.g., fire procedure).

NOTE: This branch is a screening branch that requires the analyst to determine a priori whether the logic of the procedure is ambiguous or potentially misleading even for the nominal case of the PRA scenario, or to determine whether there is a variation of a nominal scenario (nominal scenarios are those that were considered in the design of the procedures, and are therefore likely to have been addressed in training) that increases the likelihood of misinterpretation. The identification of such PRA scenarios is likely to be very difficult, however, the analyst can begin to identify these by asking "how can this be misinterpreted" for the critical steps. It is crucial to get operations staff input when addressing this branch of the DT.

In addressing this branch point, the following questions may be helpful:

a) Is the procedure ambiguous in its meaning? If the steps are not clear or lack details for the desired action in the context of the sequence of interest, then the procedure is ambiguous. A procedure may also be judged as being ambiguous if acceptance criteria and tolerances or specific control positions and indicator value are not properly specified (e.g., determine the meaning of 'adequate' in the statement "determine if flow is adequate").
b) Does the procedure contain double-negatives or overly complicated logic?
c) Are charts, graphs, or figures within the procedure difficult to interpret?
d) Does the procedure prompt a situation in which the operator is required to perform calculations or make other manual adjustments without the aid of worksheets?

➔ If the analyst answers Yes to any of these questions, the YES branch may be appropriate.[11] Otherwise, this CFM is not relevant and the NO branch should be taken.

Branch Point 2: Workload

Definition: This branch is intended to distinguish between scenarios where a distraction is present from those where it is not a concern.

[11] Although mistakes may still occur in reading the procedures even if they are well written, these errors are covered in the CFM of "misread or skip step in procedures".

Explanation: When distraction as a result of high workload is high there is an increased chance of misinterpreting written information. Time available, compared to workload, is also a factor in this branch. The high workload or time pressure may serve as a distraction so that the operators are unable to fully focus attention on the procedure or develop the correct mental model of the plant system and increases the likelihood they will incorrectly interpret the procedures. Therefore, determining if the procedure must be read and interpreted during a period of high workload (e.g., while the operators are still in the process of determining the plant status, or while there are several alarms or tasks that need attention) is important. To answer this question, the analyst must have an understanding of where this activity fits in with all the other crew activities that are coincident. Therefore, the response is driven by the qualitative analysis, and will depend on the thoroughness of that analysis. In terms of the workload categories, the fact that this CFM is only analyzed when the procedure is determined to be open to misinterpretation implies that W5 and possibly W1 are a given. The workload categories W2, W3 and W6 are also applicable.

Whether workload is low or high has to be measured against the norm, which to an outside observer might be thought of as high workload, but to the operators, might be considered nominal for that scenario (e.g., what they are accustomed to in training).

Therefore, in this case, the purpose of this branch point is to determine whether there are factors, either time pressure or coincident tasks that act as exacerbating factors.

In addressing this branch point, the following questions may be helpful:

a) Does the need to read and interpret procedural guidance occur at a time of high workload (e.g., while the operators are still in the process of determining the plant status, or while there are several alarms, indications, or tasks that need attention)?[12]
b) Is the time available close to the time required (i.e., little time margin)?

➔ If the answer to either question is true, the HIGH branch should be taken. Otherwise, take the LOW branch.

Branch Point 3: Training and Experience

Definition: This branch determines whether there is specific training and/or experience on the scenario.

Explanation: Training and experience primarily serve as compensatory factors, particularly if they help to address holes in the procedures (e.g., determine the meaning of 'adequate' in the statement "determine if flow is adequate") or areas that might lead to confusion. The compensatory factors will be different depending on the path so far. For example, if the procedures are known to be poorly written or to be confusing, training and/or experience may help to provide some compensation. Furthermore, more mental energy given to the task of interpreting the procedures - because the significance of the decision that is based on interpreting the procedures correctly is given a high priority compared to the other tasks being performed coincidentally - will help to compensate for difficult to understand procedural guidance.

To address this branch point, the analyst should answer the following:

a) Are the procedures known to be poorly written or confusing AND the training and/or experience provide some specific compensation?

[12] To answer this question, the analyst must have an understanding of where this activity fits in with all the other crew activities that are coincident. Therefore, the response is driven by the qualitative analysis, and will depend on the thoroughness of that analysis.

b) Is the significance of the decision that is based on interpreting the procedures correctly given a high priority compared to the other tasks being performed coincidentally?

➔ If the answer to *either* of these questions is NO, the LTA (less than adequate) branch should be taken, otherwise the GOOD branch may be taken.

Branch Point 4: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.15. The following is additional guidance specific to this CFM.

Taking credit for recovery may be possible when the following conditions are met:

1. Misinterpretation of the procedures could be modeled as the operators not performing the required function (error of omission), or as an error of commission (e.g., transfer to incorrect procedure, or initiate incorrect response). In either case, what is happening at the plant subsequent to the error has to be understood.
2. It has to be established that the operators are continuing to monitor the plant status in accordance with their procedures and the subsequent procedure steps reinforced by training indicates that their earlier response is not appropriate.
3. Furthermore, the operators must receive feedback from the plant. This feedback would need to be strong enough that it would lead them to either revisit the earlier misinterpreted procedural guidance, consult other procedural guidance that would direct them correctly (e.g., a fold-out sheet or critical function status tree, etc.), or to successfully correct their response in some other manner.

If there is no clear guidance that they should do this, no recovery should be credited.

5.2.8 RP-2: Choose Inappropriate Strategy

5.2.8.1 Definition of CFM

For this CFM, the crew has entered the correct procedure and is presented with more than one alternative for how to proceed. The crew chooses the wrong alternative, leading to the HFE. This CFM assumes the crew has the correct mental model for the scenario up until this point (i.e., knows what function(s) needs/need to be restored).

5.2.8.2 Applicability

This CFM is applicable where the crew has choices in a procedure for how to execute their response. Furthermore, it assumes that a deliberate choice is made. This CFM also covers cases where there is judgment left to the operator (e.g., external events, implementation of SAMGs). Alternatively, a decision to try to restart a system and fail to transition to a guaranteed success path in time would not be treated under this CFM; rather, it would be treated under the CFM for 'delay implementation'. For example, Westinghouse functional restoration procedure FR H-1 includes steps to try to restore feedwater until the cue for initiation of feed and bleed is reached. To apply the delay response, the operators know which the correct strategy is, but choose to hold off. This CFM, on the other hand, is an incorrect choice of strategy.

Strategy choices may be quite common, although they can be of different types. For example, the BWR procedures frequently say something like: "provide make up using one of the following systems…" In this case, as long as the systems are operable, any one of them would lead to success and, while there is a preferred order that is emphasized in training, it wouldn't matter to the PRA if the order were not strictly followed. The crew might be more comfortable using one system rather than another because it's more controllable (RCIC rather than HPCI for example when the conditions allow it). If, however, the scenario progresses such that the choice of one system over the other causes failure of the response required by the PRA scenario, then that would be covered under this CFM. For example, if the procedure calls for make up using

system that are not hard piped, then success may rely on choosing a system that can be aligned in a timely manner.

Other choices may involve methods of controlling a function, such as cooldown and depressurization where choosing a specific rate of cooldown can be identified as a specific strategy. Usually, when a rapid cooldown is required the procedure would give guidance to exceed the “normal” cooldown rate. A reluctance to do this would be a problem if, by not using the accelerated rate, a failure of the required response would result, i.e., the HFE occurs. The qualitative analysis of the HFE would have to identify this as a potential failure if it were indeed the case. For this case, one could postulate that the most relevant PIF would appear to be reluctance associated with the fact that rapid cooldown is not good for the plant in general. However, this would be a deliberate violation of the procedure and probably should not be addressed by this CFM.

Another example occurs in PWR SAMGs in which the feeding of a hot, dry SG may result in a tube rupture with a potential for consequent releases. Therefore, restoring secondary cooling may be at the expense of sacrificing a release barrier. The operators may be reluctant to restore SG feed even though it would be a better strategy in the long term.

This CFM may not be used often during full power, internal events Level 1 PRAs, but will likely be more relevant in Level 2 PRAs and more complex analyses such as those involving the use of SAMGs.

5.2.8.3 Development of Decision Tree

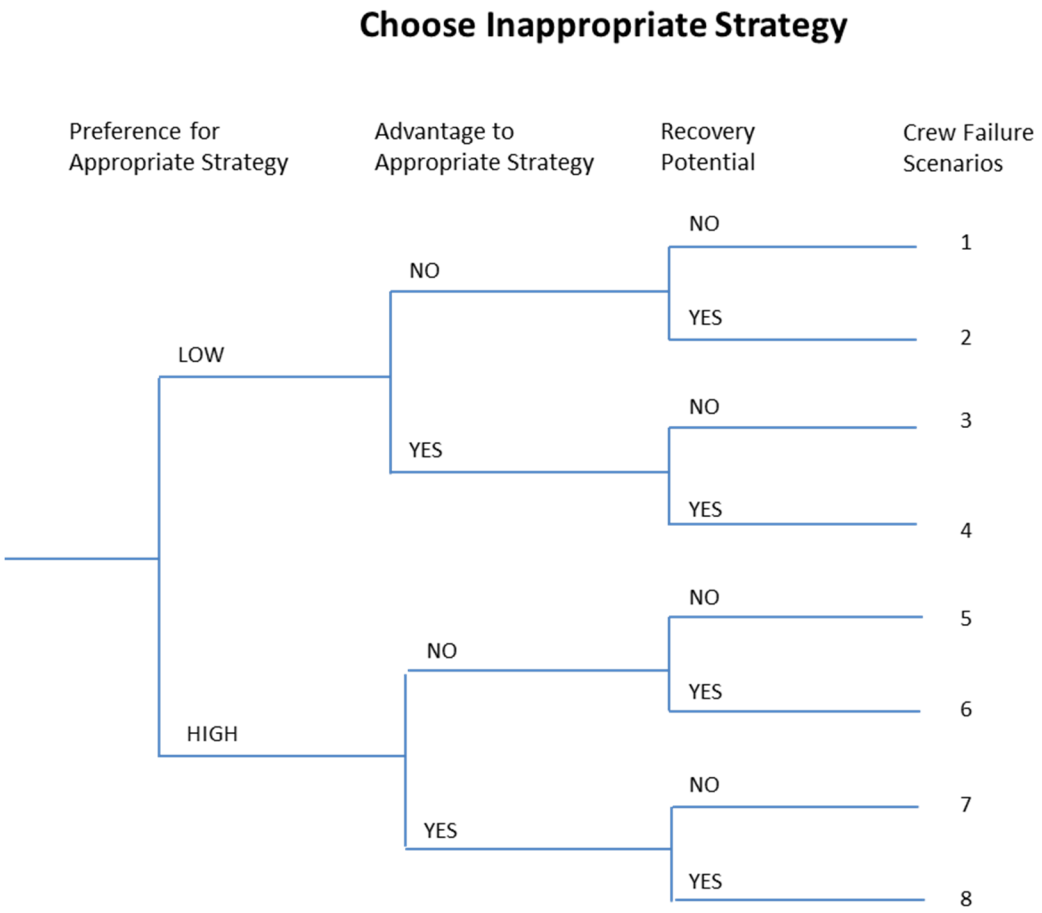


Figure 5-8. Decision Tree for CFM 'Choose Inappropriate Strategy'

Branch Point 1: Preference for Appropriate Strategy

The branch point ascertains if the crew has a strong preference to choose one option (an inappropriate one for the scenario) over the appropriate alternative. The preference for one solution will be influenced by the crew's comfort level in performing the response. A higher level of comfort with the appropriate (i.e., the correct one from the plant perspective) response would lead the crew to choose that option over the other alternatives presented. This CFM assumes that the crew has the correct plant status assessment and knows what critical safety functions need to be addressed. Therefore, a big factor in choosing one option over another will be the comfort the operators feel in applying that option. For example, if the crew has less training on, or experience in, applying the correct response, they may exhibit reluctance and a lack of confidence in their ability to apply it over the alternative response.

In addressing this branch point, the following questions may be helpful:

a) Is the appropriate response trained more regularly or experienced more often so that the crew would exhibit a preference to enact it when given the choice between the alternatives?
b) Are the operators trained in the appropriate strategy that emphasizes its significance despite any potentially negative consequences? This is particularly true for those cases where not

adopting the strategy could be regarded as a violation, e.g., not cooling down at the maximum rate.

c) Is the correct response no more complicated to apply than the incorrect response?

➔ If the answer to all of these questions is Yes, take the HIGH branch. Otherwise, take the LOW branch.

Branch Point 2: Clear Advantages to Appropriate Strategy

The purpose of this branch point is to determine whether there are considerations related to the appropriate response that interfere with the operators choosing that response. For example, if the strategy that is required for success (by the PRA success criteria) has a downside, such as it could have financial ramifications for future restart, or indeed is counter-intuitive in that it bypasses one of the primary boundaries (e.g., containment venting, although that decision would involve more than the control room crew), then the crew might be hesitant to choose that strategy.

In addressing this branch point, the following questions may be helpful:

a) Are there competing priorities that make the appropriate response appear to the operators to be less attractive than an alternative?

b) Is there a downside to the appropriate option that may not be apparent for the alternative that would bias the operators to choosing the inappropriate alternative?

c) Is there a mismatch between the procedures, policies and practices such that the inappropriate response may appear to be a more attractive response?

➔ If the answer to any of these questions is Yes, the NO branch should be taken. Otherwise, take the YES branch.

Branch Point 3: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.16. The following is additional guidance specific to this CFM. Recovery of this CFM is possible if the crew monitors the response following initiation of the action and recognizes that the strategies need to be reassessed.

5.2.9 E-1: Delay Implementation

5.2.9.1 Definition of CFM

The crew, having formed a correct plant status assessment in terms of understanding the nature of the plant disturbance and the critical safety functions that need to be controlled or restored, and knows what action needs to be taken, delays the implementation of the action to the extent that the response is not successful (i.e., the HFE occurs).

5.2.9.2 Applicability

As indicated by the definition, this CFM is applicable when the successful response is the initiation of the appropriate action at or before a critical point (which may be dictated by time or by a specific parameter value, e.g., CST level). Note that the PRA success criterion for the response requires initiation before a critical state is reached, often related to the onset of core damage, and this may well be beyond the state corresponding to the parameter value given in the procedure. One of the critical tasks of such a response involves monitoring the parameter that provides the final cue to begin initiation. There is often some margin built into the procedural guidance. A failure to follow this guidance, if performed willfully, would be a violation of a strict compliance with a procedure, even though the operators might feel they could justify it.

While the two CFMs associated with monitoring have the same effect in that they result in the initiation of the response being delayed beyond the time at which it is successful, this CFM is distinguished from “Critical Data not Checked with appropriate frequency” because the underlying cognitive mechanism is different, and therefore the PIF characteristics that enable this CFM are different. This particular CFM represents a deliberate delay rather than missing the cue. The boundary condition for this CFM is that the crew has successfully monitored the parameter and knows that the critical value specified in the procedure has been reached to perform the action, but there is perceived to be margin such that the action can be delayed to pursue another course of action.

This CFM is meant to capture those crew failure scenarios that result from: 1) delaying an action because it is hoped it can be avoided since, for example, it is an action for which the economic consequences are unfavorable and/or 2) incorrectly assessing the time to complete the action or the time available (e.g., believing that there is a margin of available time relative to the procedural directions).

5.2.9.3 Development of Decision Tree

The DT is developed on the basis that the following are reasons for delaying implementation of the action.

One reason for delaying implementation would be believing that the respective function can be achieved by recovery of a system that normally performs that function without resorting to the action (e.g., believing AFW can be restored in time to prevent going to feed and bleed). The analyst needs to identify whether there are alternate, more desirable success paths for the HFE. Note that the existence of alternate potential success paths is also addressed in the CFM “Critical data not checked with appropriate frequency” although its impact is different in that it is considered to be a factor that distracts from the monitoring activity. For the current CFM, this is related to the crew’s belief that, even though they have reached the point where they should be taking this action, they are on the brink of success with the alternate approach. An important consideration here might be the belief that they have some margin, even at the “last” minute according to the procedure.

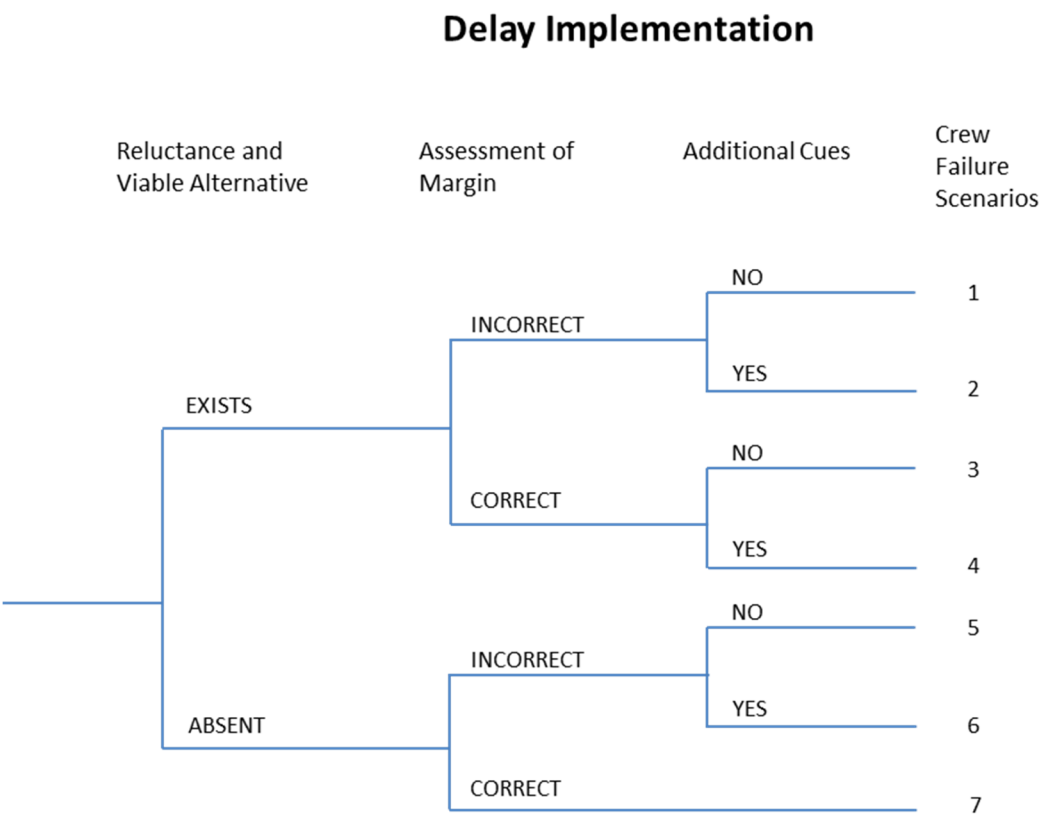


Figure 5-9. Decision Tree for CFM 'Delay Implementation'

Branch Point 1: Reluctance and Perceived Viable Alternative

Definition: This branch point is concerned with whether there could be a reason for the operators not to want to perform the response as required.

Explanation: Some required responses are considered last ditch responses and are detrimental to the restoration of the plant to full power operation. Such responses include initiation of SLC (BWRs), initiation of F&B (PWRs), or makeup with non-pure water sources (e.g., SW or Fire water). This branch addresses whether the response is of this nature. However, since it is a valid, proceduralized response (consistent with the ground-rules adopted for this version of the model) the crew would have no reason to delay implementation unless they believed there was another viable alternative to taking this action. One of these is the recovery of a primary means of achieving the function. If the plant philosophy with respect to procedure following is to carry out the required actions without delay, the analyst may assume that there is no reluctance by the crew. However, if this philosophy does not exist or is not emphasized, then the analyst must consider if the crew felt there was a downside to the response (e.g., economically because of prolonged downtime) or if there is an expectation that recovery is imminent.

In addressing this branch point, the following questions may be helpful:

a) Does the plant philosophy allow operators to exercise discretion in the pace with which they carry out procedures (as opposed to requiring operators to carry out required actions without delay)?

AND

b) Is there a downside to the response, e.g., economically because of prolonged downtime or damage to the plant? (Reluctance)

AND

c) Is there a perceived viable alternative (i.e., an expectation that recovery is imminent)?

➔ If the answer to all three points (a, b, and c) is Yes, then follow the EXISTS branch. Otherwise, take the ABSENT branch.

Branch Point 2: Assessment of Margin

Definition: This branch point questions whether the crew has an incorrect assessment of the operational margin (e.g., as measured or indicated by pressure, level, temperature) so that they think they can delay implementation longer than they actually can.

Explanation: In addition to reluctance, another factor that could play into delaying implementation is the crew thinking they have more time to complete the response than they actually do. In other words, the crew has an incorrect assessment of the time margin based on their understanding of the scenario knowing that, if the point of implementation is tied to a specific parameter value, the procedure would have been designed to provide adequate margin. However, there may be some plant conditions for which the crew's knowledge base does not lend itself to the correct assessment. The PIFs addressed here are those related to the circumstances under which an incorrect assessment of time margin is possible. The crew's knowledge base derives from training and, to a lesser extent, experience. However, actions in EOPs are typically only included if they are feasible. Thus, it is expected that adequate time is generally available and usually the lower branch (i.e., 'correct assessment') should be taken. Therefore, if the scenario is incompatible with the training such that either the training does not adequately prepare the crew in understanding the time margin related to the procedural directions or the specific scenario involves a time margin that is significantly less than those trained on, the upper branch would be taken in this tree.[13]

This is more likely to be a significant factor when combined with a reluctance to take the action reinforced by the possibility of avoiding taking the action, i.e., the upper path from the prior branch point. A strict compliance with the procedures reduces the significance of this factor considerably.

In addressing this branch point, the following questions may be helpful:

a) Is this scenario incompatible with those addressed in training and does the training fail to extend to understanding the (time) margin incorporated in the procedural directions?
b) Does the specific scenario involve a time margin that is significantly less than those typically trained on?

➔ If the answer to *either* of these questions is Yes, the INCORRECT branch should be taken. Otherwise, the CORRECT branch should be taken.

Branch Point 3: Additional Cues

Definition: This branch questions whether there are additional cues that refocus the crew on the need to begin the execution expeditiously.

Explanation: The existence of an alarm related to the initiation of the action can act as a potential recovery for all paths through the trees by redirecting the crew's attention. Also,

[13] Variants of PRA scenarios such as this are not often modeled. The HFE would typically be evaluated for the nominal conditions. However, should there be a subcontext (equivalent to error forcing context [EFC]) for which the likelihood of a negative PIF such as this one is significant, a separate HFE could be defined to capture these EFCs in the PRA model.

another crew member responsible for oversight (e.g., following the CSFSTs) might reinforce the need for immediate initiation. An example of an additional cue is where the “low” level might be the primary cue for a given action, but there is an additional alarm on “low, low” that would remind the crew.

Note that the amount of credit afforded to this alarm could be different for the path encompassing a reluctance to carry out the action as compared to no reluctance but the incorrect assessment of time margin path because the reluctance involves a cognitive mechanism that could prevent recovery.

Apart from the alarm, no explicit recovery is modeled here because, by definition, the delay has to be significant enough that the function has failed.

In addressing this branch point, the following questions may be helpful:

a) Are the alarm or additional cues salient?
b) Is the alarm (or other cue) and its importance emphasized in training?
c) Is the philosophy of the plant to respond immediately to this alarm or cue?

➔ If Yes to *any* of the questions, then the YES path should be taken. Otherwise, the NO path should be taken.

5.2.10 E-2: Critical Data Not Checked with Appropriate Frequency

5.2.10.1 Definition of CFM

This CFM represents a failure to monitor a critical piece of data so that the cue (e.g., a specific parameter value) for the transition to another part of the procedures or the initiation of a required response is missed. This is invoked contingent upon the crew having recognized that the data needs to be monitored, and belongs in either the plant status assessment or the execution phase of response. It is a special case of failing to initiate a response, but has a different cognitive mechanism than the CFM ‘fail to initiate execution’, since that is more related to forgetting.

5.2.10.2 Applicability

This CFM is applicable to a monitoring activity where the instruction (either procedural instruction or trained expectations) to transfer to a different part of the procedures (e.g., transition to a functional restoration procedure using critical safety function status trees or a continuous action statement) or initiate some response (e.g., switchover to sump recirculation) is conditioned on a critical value of some parameter that is trending and expected to be trending rather than remaining static (e.g., RWST level). This CFM is expected to occur when the crew has an incorrect understanding of the rate of change of the parameter such that the monitoring strategy is deficient. Assessing the trend incorrectly may, therefore, be a contributing factor for this CFM. This CFM is typically expected to apply to a single, dynamic datum. The purpose of this CFM is to capture those cases of missing a critical value of a parameter and, therefore, not responding in time as reflected in the definition of the HFE. This CFM would be used for data collection that occurs as part of routine scanning or board monitoring only if the qualitative analysis indicates that such an activity is an essential part of the required response.

An example HFE in which this CFM is applicable is the switchover to recirculation, and this CFM applies once the operators have determined that they have a LOCA and that switchover to recirculation is necessary to prevent pump cavitation, and that they need to monitor the RWST level; the initiation of the actions to switchover is conditioned on RWST level. Another example is the HFE for initiation of SLC in response to an ATWS (BWR). The initiation of SLC is keyed to suppression pool temperature which is the monitored parameter. Failure would correspond in

both cases to missing the critical value to such a degree that the function (cooling in the first case, and reactivity control in the second) is lost.

5.2.10.3 Development of Decision Tree

This CFM is intended to be used when the crew know that they have to monitor a parameter until it reaches a key value at which time a response is required. The way in which the monitoring is done is an important factor. An optimized monitoring strategy will lessen the probability of failure. Other factors that could affect the probability of failure are the workload and the expectations concerning the rate of change of the parameter. In many cases, the critical value of a parameter may be reinforced by or shortly preceded by an alarm. The occurrence of such an alarm would act as a recovery factor, since it would be reminder.

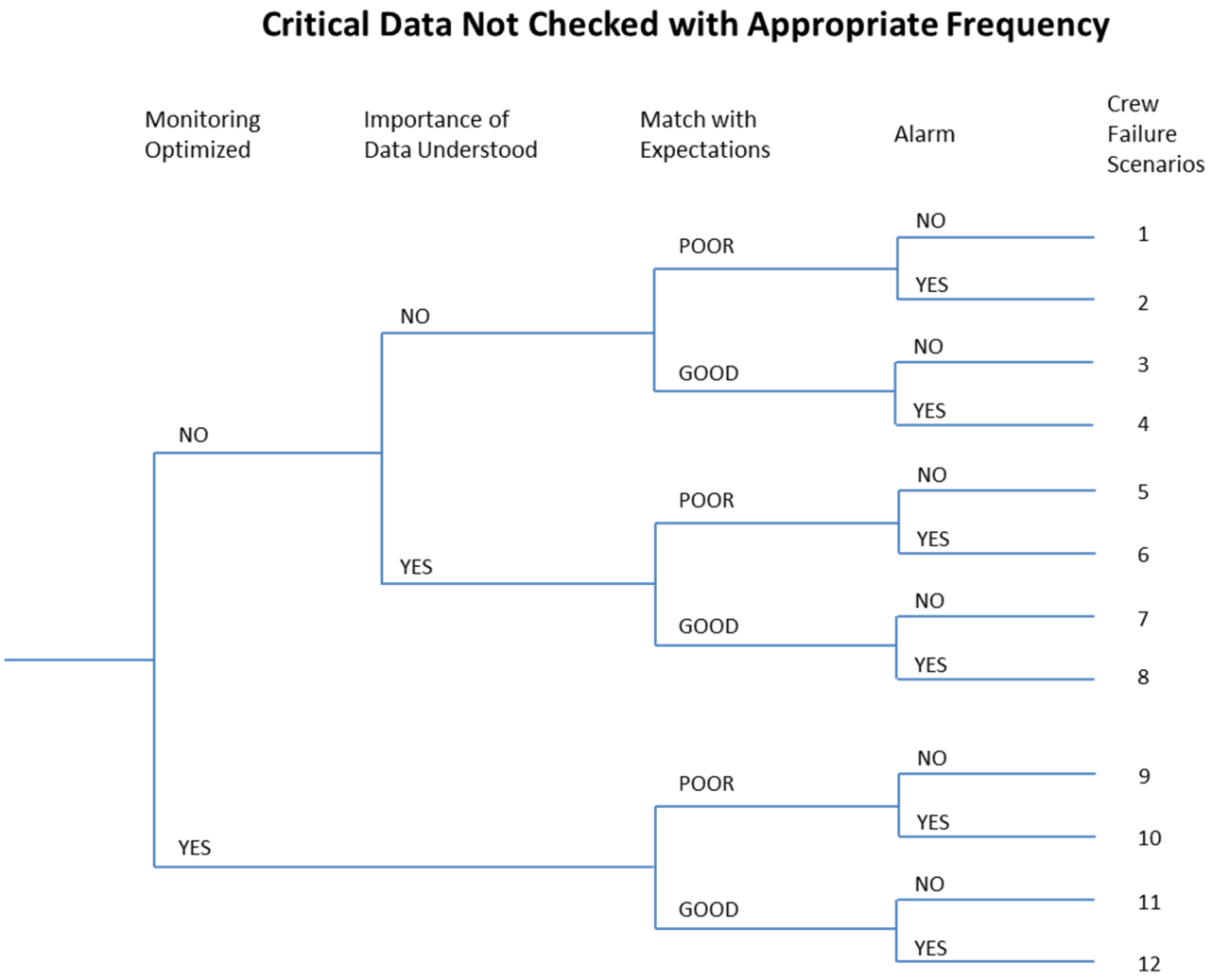


Figure 5-10. Decision Tree for CFM 'Critical Data Not Checked with Appropriate Frequency'

Branch Point 1: Monitoring Optimized

Definition: This branch distinguishes between those cases where the monitoring is such that the resources allocated for the activity of monitoring the parameter in question are considered optimal from those where this is not the case.

Explanation: Two cases may exist such that either there is a dedicated crew member assigned to monitor the particular parameter or there is a crew member monitoring the parameter while performing other tasks. The former case can only exist when the workload is not high, or at least the workload is such that an operator can be dedicated to the task. In addition to determining if a crew member is singularly responsible for this monitoring task, the analyst should also determine how the monitoring is done. Again, two cases may exist such that either the monitoring is done continuously or periodically. If the parameter is only monitored periodically, there is the possibility that frequency of checking is miscalculated and the crew member misses some important change.

On the upper branch, monitoring is ad hoc or performed as the crew member gets to it. On the lower branch, the monitoring is optimized with a dedicated operator for whom it is the only function that operator is concerned with at the time.

In addressing this branch point, the following questions may be helpful:

a) Is there a crew member assigned to watch the key parameter with no other tasks being performed by this crew member?
b) Is the key parameter monitored continuously or are the operators trained on how to adequately monitor the key parameter to ensure it is monitored often enough?

➔ If the analyst answers No to *either* of these questions, the NO branch should be taken. Otherwise, take the YES branch.

Branch Point 2: Importance of Data Understood

Definition: This branch point is intended as a compensatory factor for the case where the monitoring is not, or cannot, because of workload for example, be optimized and relates to the awareness of the crew that the function for which the monitoring is being performed is one that needs to be performed when conditions require it.

Explanation: In the case that the monitoring is optimized it is assumed that the importance of the data being monitored is recognized. Therefore, this branch is not included on the monitoring optimized branch. However, in the case that monitoring is not optimized, it is assumed that the operator could be performing multiple tasks. Therefore, the analyst must determine that the training and procedures stress the significance of this data monitoring task and afford it a higher priority than the other tasks the operator may be performing at that time. This can be determined by understanding how the operating crew would be working in the situation addressed by the HFE in question.

The upper branch corresponds to the case where there is no motivation to improve monitoring, and the lower branch to the case where the monitoring is considered to be significant enough that it is given a high priority among the other tasks that may be being conducted concurrently.

The following question is intended to assist the analyst in addressing this branch point:

a) Are the operators trained on the significance of the parameter so that the monitoring task is given a high priority among the other tasks they may have to perform, so that they at least to check the parameter frequently?

➔ If the analyst answers No to this question, the NO branch should be taken. Otherwise, take the YES branch.

Branch Point 3: Match with Expectations

Definition: This branch addresses the issue of whether the training and experience of the crew are sufficient to establish an appropriate monitoring regime.

Explanation: This branch addresses the potential limitations of the mental model being used by the operators to perform the monitoring. It is assumed that the operators have the correct mental model of the plant status and that they are aware of the need to monitor this particular parameter. However, the operators may have an inaccurate mental model of the rate of change of the parameter.[14] The mental model regarding the rate of change of the parameter sets the operator's expectation regarding how quickly the parameter would change, and therefore, how frequently the parameter should be checked. As for the previous branch, it may not be necessary to ask this question for the case where the monitoring is optimized. Training would have focused on the rate of change of the parameter for one or more nominal cases. Therefore, factors that influence this issue are the frequency of training and the nature of the training and whether they are sufficient to give the operators the correct understanding of the rate of change of the parameter for the specific PRA scenario. One factor that could have a negative impact is the effect of equipment failures not addressed in the training scenarios that make the plant parameters behave differently than the training scenarios and/or operating experience would predict. Identification of these "deviation" scenarios may lead to a restructuring of the PRA model.

On the GOOD branch, differences in the rate of change are either not relevant, because there is no firm expectation other than the trend, or the training allows for a range of expectations. On the POOR branch, the context has to be such that the training/experience has produced some sort of bias that would distort the monitoring regime. For the monitoring optimized scenarios, this may well be an irrelevant question.

In addressing this branch point, the following questions may be helpful:

a) Is training on the correct monitoring scheme for this parameter in the PRA scenario for which this HFE is being evaluated relatively *infrequent* such that the operator is unable to learn the correct rate of change for the parameter?
b) Might the key parameter be affected in novel ways that are not covered in the training that might affect the rate of change?

➔ If the answer to *either* question is Yes, the POOR branch should be taken. Otherwise, take the GOOD branch.

Branch Point 4: Alarm

Definition: In this context, the alarm is considered as a reminder that the critical level of parameter has been reached.

Explanation: An alarm that is related to the parameter and reminds the crew to attend to the function is a powerful recovery.

In order for the alarm to be credited as a potential recovery mechanism, the analyst should answer the following:

a) Does the alarm pertain to the parameter being monitored?
b) Is training on the alarm focused so that it is recognized as important?
c) Is the alarm's significance with respect to the action required understood?

[14] Although similar to "match with expectation" from other trees (e.g., Decide to Stop Collecting Critical Data), the key difference in this case is this refers to a local mental model (i.e., to a specific parameter) rather than to the overall plant status.

➔ If the analyst answers No to *any* of these questions, then recovery cannot be credited and the NO branch should be taken. Otherwise, take the YES branch.

There is no additional recovery option offered because it is assumed that the failure to initiate allows no recovery. This does imply that the monitoring frequency has to be sufficiently at odds with the plant state that the function will fail. Because of this, this CFM is likely only to be significant for second order responses, i.e., those related indirectly to the critical safety functions. A response like failing to depressurize (BWR) or failure to switchover to recirculation (PWR) are so important that they will fall onto the YES path at the first branch.

It should be noted that for a task for which this CFM applies, it is likely that some form of communication between crew members is required and, therefore, the CFM 'critical data miscommunicated' will be included in the assessment. The information being incorrectly processed is another potential CFM.

5.2.11 Action CFMs: Fail to Execute Action / Fail to Correctly Execute Response

5.2.11.1 General Definition of CFM

The crew fails to execute the response as required. This includes the classic error of omission, and does not specify how or why the execution is not performed. This definition may broadly be interpreted to include any failure to even start the process; however, a deliberate decision not to start an action is covered by the response planning CFMs. A failure to start caused by a slip, on the other hand, could be included here. However, perhaps the more significant contributions come from the errors of commission, i.e., not performing the execution correctly so that it fails to achieve its goal.

These CFMs are conditional on the crew having identified the correct (physical) response and decided to initiate the response.

There are two categories for the general classification of Action CFM:

- Fail to initiate execution
- Fail to correctly execute the response, which is applicable once the action has been initiated but the execution is not performed correctly in such a manner that the goal of performing the action is not achieved, i.e., the HFE occurs. There are a number of ways of failing to perform a response correctly that include not completing all the required actions in time, as well as performing some of the steps incorrectly, or performing the steps out of sequence when the ordering is critical. This CFM, therefore, is a broader class that includes errors of omission (the former) and the potential for errors of commission.

5.2.11.2 Applicability

[NOTE: In a PRA model that doesn't explicitly model the consequences of an EOC, the effect would be modeled the same for both categories of the action CFMs. However, the potential for recovery is undoubtedly dependent on what happens to the plant when the incorrect action is taken. This could probably still be assessed off-line, i.e. outside the PRA model. To model errors of commission it is necessary to identify the specific errors that are made in the execution, since the consequences of the errors need to be explicitly understood if they are to be modeled. This requires a more thorough investigation of the sequencing of actions and errors.]

For both categories of this CFM, the possibility that the crew has taken too long to reach the correct plant assessment and determine the correct plan of action, and therefore, not allowed time for implementation, should be covered in CFMs within the SA phase and RP phases. Therefore, it is the concerns about timing in implementing the action, given the time available is in principle sufficient, that would be addressed with these CFM categories, mainly as it impacts

the opportunities for and the feasibility of recovery. These CFMs, and particularly the failure to execute correctly, are most likely to be significant contributors in a time-constrained situation where the potential for recovery is lacking. The identification of time-constrained HFEs is therefore important. Those scenarios where the time is just sufficient to make the correct plant assessment, choose the correct response and execute it are relatively easy to identify. The action CFMs would be assessed on the assumption that the plant status assessment and the response planning took the nominal time. For those actions for which the total time window is more than just adequate, the action CFMs (and particularly the possibility of recovery) should be assessed on the basis that the plant status assessment and response planning took the nominal time. While the CFMs for the SA and RP phases do include the potential for recovery, which would reduce the time available for execution, the likelihood of those scenarios is expected to be considerably lower than the nominal. Therefore, to a first order approximation, this contribution is neglected. Allowing for this would be possible in a more dynamic framework. The effect of considering these paths, and therefore decreasing the potential for recovery in the execution phase, can be investigated once the complete set of decision trees has been established.

Both the following CFMs are included whenever the task for success of the CRT path includes an execution step or steps.

The CFM “Fail to initiate execution” is probably best characterized as a lapse, i.e. forgetting to begin the response.

The CFM “Fail to correctly execute the response” could address such errors as reversing steps in the action when the ordering matters or taking too long as a result of getting hung up at some point. There are numerous ways that the action can fail. However, the intent is to model these in the same way as the other CFMs, using decision trees. It is assumed that the response has been initiated.

For this “Fail to correctly execute the response” CFM, it makes a difference whether the task that has to be performed is a simple manipulation of a number of steps to change the status of a system, or whether it is a continuous action, such as cooldown and depressurization following a curve for the pressure and temperature. The latter case involves a continuous evaluation of the plant status and making adjustments as necessary and is referred to as a control action. This task, therefore, involves potentially more cognitive activity although it is in the nature of monitoring, understanding the change in parameter values and making adjustments as necessary, and generally falls into the category of skill of the craft. However, even for the former case, it is necessary to address the issue of recovery as a result of feedback from the plant as the manipulations are made. Because the nature of the tasks is different, it is useful to develop different trees to address these two cases, but a tree for addressing control actions has not yet been developed.

5.2.11.3 Development of Decision Trees

Different decision trees are applicable for each of the following:

- Failure to initiate execution (a simple error of omission)
- Failure to correctly execute response
  - Simple Action
  - Complex action
  - Control action (undeveloped)

Using decision trees to assess these actions moves the modeling from the detailed task analysis level (à la THERP) to a more holistic functional level. This is the primary reason for creating different trees for tasks with different characteristics. Control actions in particular have

not been modeled well in the past – typically they have been modeled only as errors of omission.

5.2.11.3.1 E-3: Failure to Initiate Execution

Entering this decision tree, the crew has correctly diagnosed the plant status and made the decision to execute the action. This CFM is best characterized as a lapse, i.e. forgetting to begin the response, and should not be confused with the CFM “Delay Implementation” which is a strategic decision by the crew to delay execution of a needed action.

This is a simple tree, focusing on the workload and nature of the task. Although HSI may also be considered relevant, it is not considered an issue here since the decision has been made that the action needs to be performed (success in PSA and RP). That is, if HSI were an issue, it would likely have already had an impact accounted for in one of the earlier CFMs.

The first branch is related to the immediacy of the task. Of concern here would be questions like, does the responsible crew member act immediately to perform the action or is it put on a to-do list? If it is not immediate, this would suggest that the task is not important to the stabilization of the plant and thus this situation might be more likely to be encountered later in the PRA sequence rather than in the early stages. If the response is immediate and there are no competing demands this should degrade to a lapse and get folded into the lower limit on the HEP. If the response is immediate, no other PIFs are considered.

The second branch is related to workload, the idea being identifying whether there are coincident tasks the crew has to perform that somehow diverts attention from the execution, given that the execution may in fact be delayed. For example, a new task could be initiated by a new alarm that demands the attention of the whole crew but is unrelated to the function to which the action pertains. Whether the workload is high or not in this case should be determined by understanding the nature of the PRA scenario leading to the HFE.

Finally, the possibility of recovery is included. This is most likely to come from some crew member monitoring the plant status to check whether the expected change has occurred. This may be credited if the monitoring is being performed by a crew member other than the board operator who forgot to do the manipulation. Note: Failure to communicate the need for the task is addressed in the CFM ‘Data Miscommunicated’. For recovery to be credited, there has to be sufficient time for the feedback to become evident, and that failure of the function has not occurred at that point in time. In other words, there is sufficient margin between the parameter(s) being monitored to indicate that the response has not been effective, and the time window beyond which recovery is not possible.

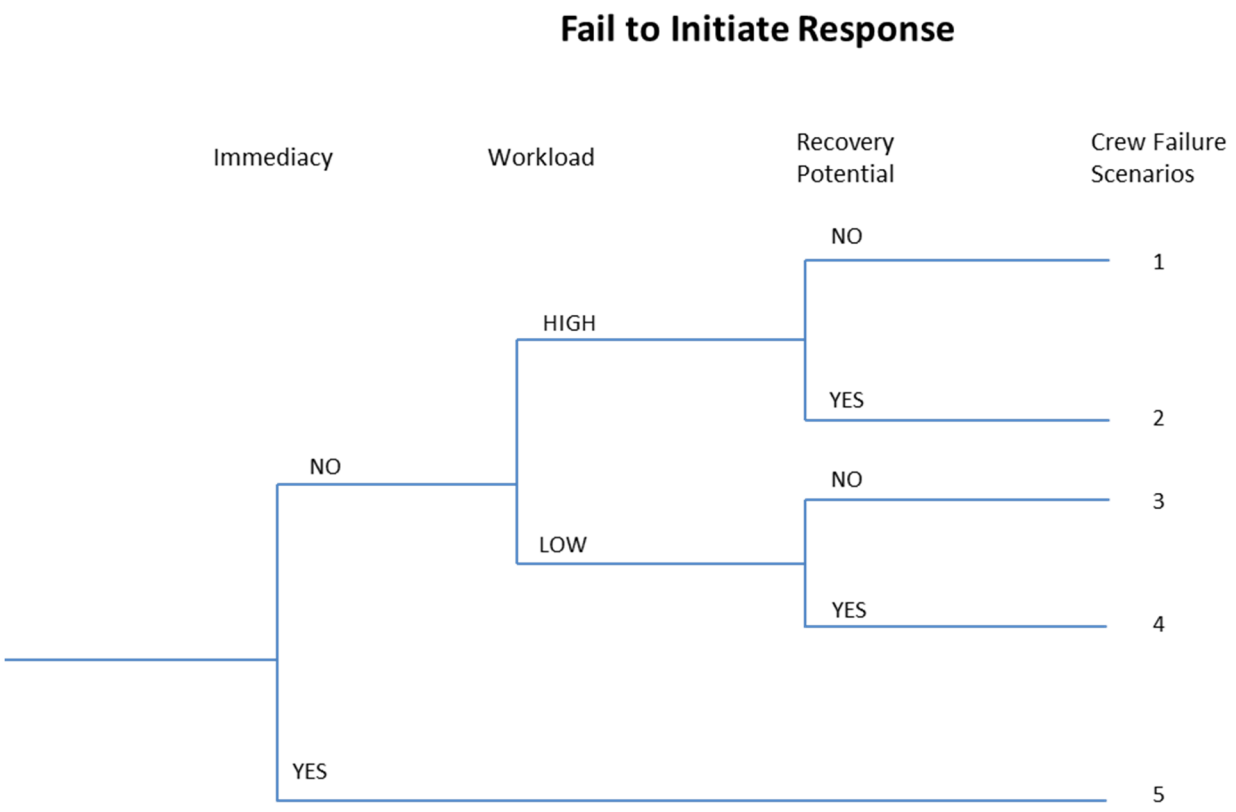


Figure 5-11. Decision Tree for CFM 'Fail to Initiate Response'

Branch Point 1: Immediacy

Definition: This branch point is concerned with the way the operators are trained to respond for the scenario in question, and in particular, to identify if this is an immediate action. Essentially, this can be thought of as "is this action on the top of the operator's mental queue"?

Explanation: The thinking behind this branch point is that if the action is to be executed immediately, there should be no reason for failing to begin to implement it, i.e., the chance of forgetting to initiate it is minimized. If there is a possibility that the response will be put on the back burner, then the chance of forgetting is increased. To some extent, workload and lack of immediacy are correlated. If the task is not immediate, i.e., the guidance or practice is to get to it when you can, this would suggest that the task is not important to the stabilization of the plant and thus this situation might be more likely to be encountered later in the PRA sequence rather than in the early stages. The execution is more likely to be immediate if it is related to restoration or initiation of a critical safety function required to stabilize the plant condition as opposed to a response that can be taken at some later time. If the response is immediate and there are no competing demands this should degrade to a slip and get folded into the lower limit on the HEP. PIFs relevant to this branch point include knowledge and training as well as available time.

In addressing this branch point, the following questions may be helpful:

a) Is the execution related to restoration or initiation of a critical safety function required to stabilize the plant condition as opposed to a response that can be taken at some later time?

b) Is the particular safety function considered (by training or procedure) to be a priority in this PRA scenario?
c) Is the timing of the scenario development such that the conditions for initiation of this action are reached before the other competing actions?

➔ If the analyst answers Yes to *all* of these questions, the YES branch should be taken; otherwise take the NO branch.

Branch Point 2: Workload

Definition: In this context, workload is intended as a potential distractor. Essentially, this can be thought of as "how long is the operator's mental queue"?

Explanation: The purpose of this branch point is to assess whether there is a distraction caused by high workload (primarily W2 but may include aspects of W3). If there are coincident tasks that the crew has to perform, they may divert attention from the execution of this action. For example, a new task could be initiated by a new alarm that demands the attention of the whole crew but is unrelated to the function to which the action pertains. Whether the workload is high or not in this case should be determined by understanding the nature of the PRA scenario leading to the HFE.

In addressing this branch point, the following questions may be helpful:

a) Does the need for this response occur when there are no other tasks or procedures being employed (or the crew does not need to respond to several things)? In other words, can the crew focus on this task instead of having multiple functions challenged at the same time?
b) Is the accident scenario such that the crew is not likely to be interrupted in the middle of their procedure to attend to another task or person?
   Answering these questions requires that the analyst develop a clear picture of the challenges to the plant as a result of the defined PRA scenario including a detailed timeline of the cues and plant condition, and the guidance that is being provided by procedures or training on how to respond.

➔ If *both* are YES, the LOW branch should be taken; otherwise, take the HIGH branch.

Branch Point 3: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.16. The following is additional guidance specific to this CFM.

Definition: This branch point addresses the opportunities for recovery. Immediate recovery, which may come from self-recovery or from peer-checks, is already credited in the base HEP. If there is sufficient time, recovery credit can be given for another crew member who is overseeing the crew (STA, TSC) and monitoring the plant status to check whether the expected change has occurred. Other recovery opportunities could arise, such as an alarm that reminds the crew of the need for the action.

Explanation: For recovery to be credited, there has to be sufficient time for the feedback to become evident, and that failure of the function has not occurred at that point in time. In other words, there is sufficient margin between the parameter(s) being monitored to indicate that the response has not been effective, and the time window beyond which recovery is not possible.

5.2.11.3.2 Failure to Execute Response Correctly

The following factors are relevant to understanding the nature of the response in order to categorize it as simple or complex and also to determine the appropriate paths through the DTs:

- The nature of the task – different tasks have different critical tasks
  - Which of the steps are critical – how many steps if performed incorrectly lead to failure?

    - Do the steps have to be taken in the correct order? Is reversal of steps critical in that it precludes recovery? An example of such a failure cause might be incorrectly starting a pump before opening the discharge valve.
    - Do the tasks have to be performed quickly?
- How the task is performed
    - Assuming that the task is performed following a procedure (as opposed to memory), is it necessary to worry about order reversal or missing a step in the procedure? Use of place keeping aids would limit the likelihood of these types of failures.
    - If the task is performed using a procedure, are there verification steps at the key actions or intermediate points (or is the verification done globally when the action is completed)?
    - Does the task allow for the performer to verify his or her action at each step?
    - Is there independent checking (probably not)?
    - Upon completion does the procedure and/or training require the operators check that the actions have been successful?
    - Does the task require crew members to communicate, one from an ex-control room location to one in the control room or between ex-control room locations?
    - Is three-way communication rule followed?
- Whether the feedback is conducive to reducing error
    - Is the feedback on correctness of actions immediate at each step or at least at each critical step in the procedure? Feedback on the correctness of individual steps cannot be relied on to eliminate or correct step reversal or missing a step. Nevertheless such feedback is indicative of a user friendly HSI.
    - If the feedback is more global (i.e., at the end of the execution), is it timely and are the indications from the plant discriminating enough to indicate that the result is not as expected?
    - Note that even though the feedback on individual actions (e.g., closing a valve) may be immediate (e.g., by observing status light change), it will not correct the closing of an incorrect valve, so questions about feedback will have to be dealt with at a more global level.
- Whether the HSI promotes high reliability
- Whether the task is familiar from training
- Whether there is a high workload

NUREG-1921 [3] provides some state-of-the-practice considerations for determining execution complexity. These factors were taken into consideration when developing the following list, which outlines issues that should be considered when deciding the level of complexity for an action. This list provides an initial assessment of complexity to help the analyst determine which of the following trees should be used.

- **Number of tasks to be completed**. If an action requires only a single step (or very few steps), can be performed by a single crew member and is supported by clear procedures (i.e., trained personnel should be able to follow them straightforwardly) or can be considered skill-of-the-craft, the action can generally be considered to be of low complexity. If, however, multiple steps must be completed, the complexity increases. This complexity may be tempered (i.e. lowered) if the execution of the multiple steps may be performed by multiple crew members working independently of what other personnel involved in the action are doing and the execution of the steps is supported by either clear procedures or the actions can be considered skill-of-the-craft.
- **Simultaneous action sequences**. If a single crew member is responsible for performing or monitoring multiple actions almost simultaneously, the complexity can be considered to be high. Likewise, if multiple crew members are required to complete an action and the steps require coordination and communication among team members to successfully compete the

action, high complexity should be assumed. This will be true when the steps must be performed in a particular sequence and when the steps involve a combination of sequential and parallel steps. Exceptions would be well-trained, EOP-based actions in the main control room (MCR) that are part of the expected response to an initiating event – but even these actions should be examined carefully for potential ambiguity and difficulty.

- **Multiple location steps**. If the execution of the action requires one or more members of the staff to visit multiple locations (either within or outside the MCR), the complexity is increased. This increase in complexity is particularly true if coordination and communication among staff members is required. Generally, if multiple locations must be visited to complete the action, high complexity should be assumed.
- **Multiple functions**. Multiple functions may need to be addressed in the execution of an action (e.g., both electrical alignment and mechanical) that will increase the execution complexity of the action. When multiple functions must be addressed, the complexity should generally be assumed to be high.
- **Accessibility of location or tools**. If there is reason to believe that a location will be difficult to reach (e.g., inadequate lighting) or tools necessary to complete the action will be difficult to retrieve or use (e.g., tools or access panel is locked and keys are not conveniently located), the complexity should be considered high.
- **Environmental factors**. Environmental issues include excess noise that may make it difficult to hear or communicate to other crew members. This factor may be especially prevalent in an ex-MCR location in which excess noise may degrade the quality, clarity or volume of the message being communicated. Other factors such as steam and temperature may also play a role and affect the ability of the operator to perform the required action.
- **Ex-MCR actions**. If the actions must be performed outside of the main control room (MCR), complexity should be considered high (i.e., the complex execution tree should be used). The ability of the crew to complete the actions reliably even though they take place outside the MCR is addressed by the DT.

A continuous control action (i.e., an action that relies on system feedback or is a series of manipulations or control tasks) may also be considered complex.

5.2.11.3.2.1 E-4: Failure to Correctly Execute Response (Simple Task)

A simple task is defined here as one which is accomplished by performing one or two manipulations, does not require following a written procedure (although there may be written guidance), and the direction may instead be a verbal instruction from the procedure reader to the board operator. Any response that does not meet this definition of simple should be analyzed using the decision tree for a complex task. Since this failure does not include the complete omission of the action, for a simple case, this could be a slip and could be exacerbated by poor HSI. Working memory should not be challenged, unless perhaps there is a high workload from competing tasks. An important factor is how the response is performed; for example, is it standard practice to check that the plant response to the action is as expected? For this to be an effective recovery mechanism, the feedback needs to be sufficiently timely to allow a check to be made on the action taken and for a corrective action to be performed. Thus, the DT addresses workload, HSI, and recovery. For the latter, the questions will address whether the protocol requires checking that the response is as expected, and that the feedback provides timely indications that corrective action has to be taken.

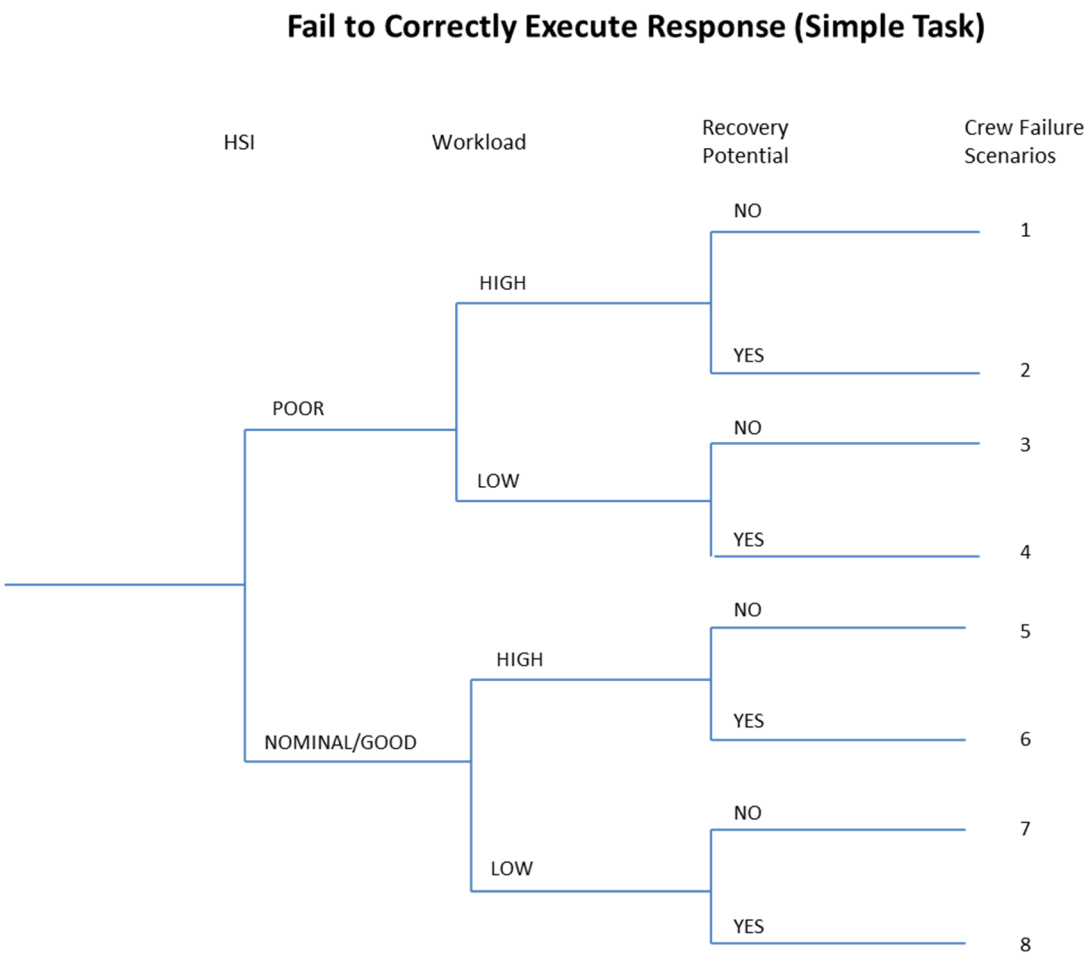


Figure 5-12. Decision Tree for CFM 'Fail to Correctly Execute Response (Simple Task)'

Branch Point 1: HSI

Definition: The aspects of HSI that are considered in this branch are those that have a direct impact on the performance of the response (i.e., task-specific HSI, not general plant HSI), and will include the indications and controls relevant to the response.

Explanation: In general, the HSI for most tasks in the control room should be well designed. The questions here list examples of poor HSI and the analyst should assess the context to determine if poor HSI exists. Also, even simple tasks taken outside the control room may suffer from poor HSI. If there is good training on this indicator, the HSI can be considered GOOD.

An example of poor HSI might include two valves identified by a long string of characters where the only differentiation is one character in the middle differs. Some human factors deficiencies include, but are not limited to, [taken from THERP [4]]:

- Poorly designed scales, and scale numeral progressions that are difficult to interpret
- Parallax problems in relating pointers to scale markings and numerals on meters
- Placement of meters above eye level, making them difficult to read
- Glare and reflections
- Too many channels of information on chart recorders

- Illegible pen tracings or symbols on chart recorders
- No warning before a chart recorder or pen runs out of ink
- Use of chart recorders where meters or digital readouts would be more appropriate (e.g., where lags in data can result in wrong decision)
- Functionally related displays are widely separated physically
- Inconsistent coding and labeling among displays
- Lack of limit marks on meters
- Meters not arranged with "normal" segments in the same relative positions (to facilitate check-reading)
- Similar controls (e.g., circuit breakers, group of valves similar in size/shape/state and presence of tags) that are densely grouped and identified only by label

In addressing this branch point, the following questions may be helpful:

a) Is the information (labels and displays) given by the HSI available, prominent, easy to read, distinctive and unambiguous?
b) Does the indicator or control follow population stereotypes (i.e., the expectation is when we turn a valve clockwise, flow will be reduced – does the control follow that expectation or deviate from it)?
c) Are the environmental conditions and physical requirements nominal (i.e., adequate lighting, no smoke, no special physical requirements, etc.)?

➔ If the analyst answers Yes to *all* of these questions, the NOMINAL/GOOD branch should be taken. Otherwise, take the POOR branch.

Branch Point 2: Workload

Definition: Workload refers to anything that might distract attention from the task such that there is an increased chance of it being performed correctly.

Explanation: Since this is a simple response, high workload refers to competing tasks that need to be done in the same time-frame (Categories W2 and W6). Time pressure is included here as part of workload. For example, for an ATWS scenarios where the breakers need to be locally tripped, it is a simple but time critical task, so the workload may be considered high for this execution.

In addressing this branch point, the following questions may be helpful:

a) Can this task be performed by a single crew member? In other words, can the crew member focus on this task instead of having multiple functions challenged at the same time?

➔ Since this is a simple task (by definition) this may not be a strong factor given that the crew has started to execute the response, and that a crew member has been designated to perform the response. However, if the answer is Yes, the LOW branch can be taken (i.e., Low Workload). Otherwise, take the HIGH branch.

Branch Point 3: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.3. The following is additional guidance specific to this CFM.

Definition: In this context the recovery is considered as taking place while the response is being executed or shortly thereafter. [*Note: this is probably the most important branch.*]

Explanation: The crew has correctly identified the plant status, followed the procedure correctly up to the point of initiating the response, and has begun implementing the required action. Therefore, it is assumed that they understand how the plant should respond. The analyst must ensure that there is sufficient time to realize the error and correct it before the function is failed.

To take credit for recovery, the analyst should assess the following:

a) The practice is to check that each of the steps has been carried out correctly AND the feedback is clear, immediate and/or timely (i.e., the crew is able to monitor the plant response and confirm that the response is as expected in sufficient time to take corrective action if necessary)?
b) If there are alarms or procedural checks that lead back to the function in question? This may provide additional opportunity to recover.

➔ If the analyst answers Yes to *either* of these questions, the YES branch should be taken. Otherwise, take the NO branch.

5.2.11.3.3.2 E-5: Failure to Correctly Execute Response (Complex Task)

A complex task is one which includes a significant number of manipulations or involves challenging cognitive activities that have to be completed successfully for overall success of the mission. Further, for a complex task, the manner in which it is performed can have a significant effect on its success. This decision tree is intended to cover a range of complex tasks, and the reasons for complexity can vary between tasks.

In order to use this DT for quantifying failure to correctly execute a complex action, the following assumptions are made:

- This CFM, in accordance with the definition, is dependent on the operators having identified the correct response and begun to execute it. In other words, they know what function they are dealing with and what the expected outcome should be.
- In order to use this DT, it is assumed that all of the actions are directed and covered by a written procedure (including ex-control room actions). While some of the basic actions may be skill-of-the-craft, the key actions are directed by procedure. If the actions are not covered by procedure, they cannot be quantified with this tree without additional justifications as to why a written procedure is not necessary.
- If the scenario is such that substantially adverse environmental conditions resulting for example from flooding, fires or seismic events, then those actions cannot be quantified with this DT. Either the actions must be quantified with another approach (e.g., NUREG-1921 for fire conditions) or the actions must be assigned an HEP of 1.0.
- The DT is intended to distinguish between HFEs where the conditions are optimal and those where they are not.

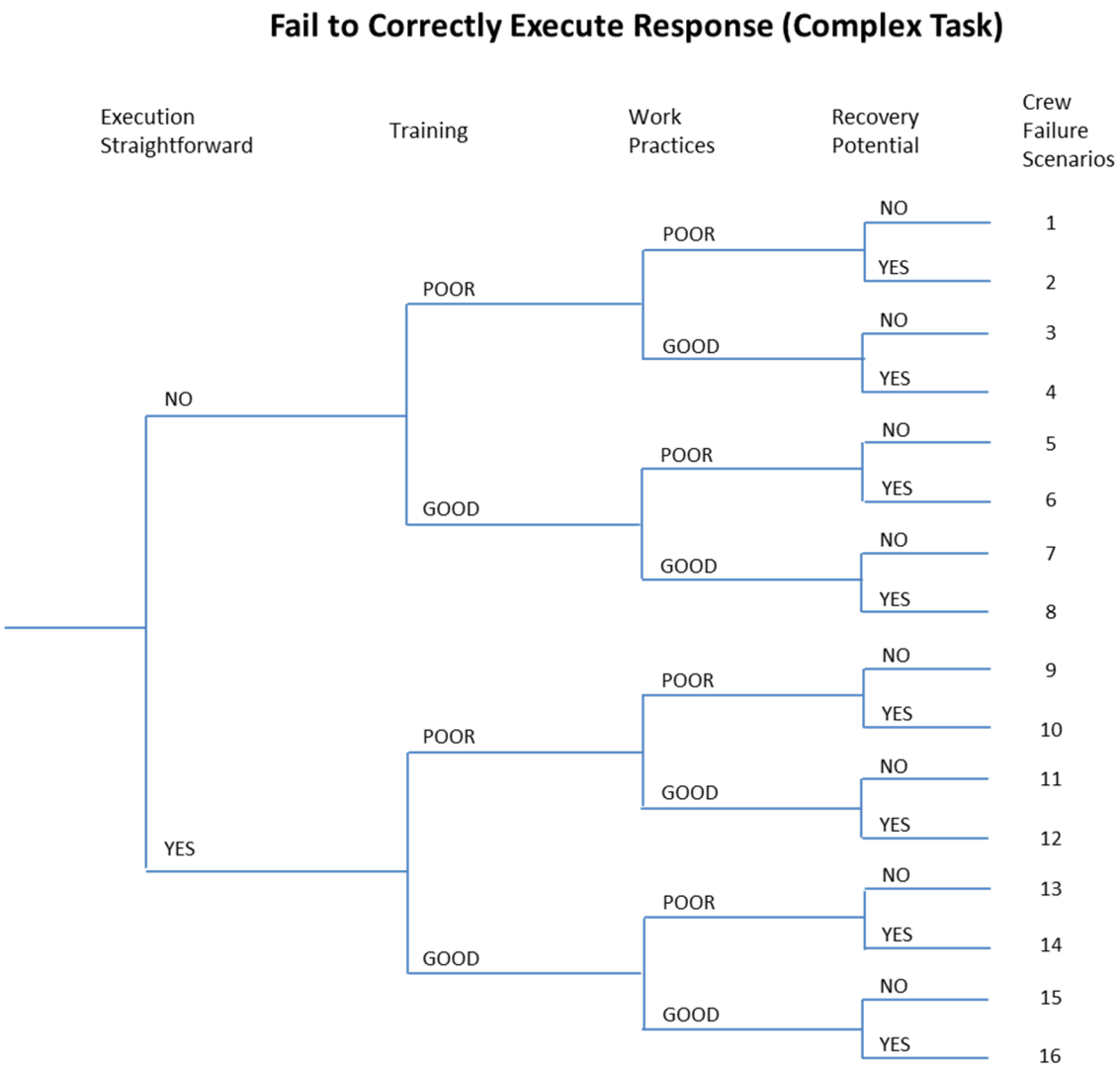


Figure 5-13. Decision Tree for CFM 'Fail to Correctly Execute Response (Complex Task)'

Branch Point 1: Execution Straightforward

Definition: Although there may be multiple tasks involved or other characteristics that make the actions complex, the individual actions (tasks) themselves would be straightforward for any licensed operator or other professional plant personnel that would be asked to perform the actions. In other words, there is nothing inherently unusual or difficult involved in performing the specific tasks. This branch is used to distinguish between tasks that, even though they are complex or are performed outside the MCR, can be expected to be performed reliably, and those for which there are task characteristics that can be conducive to error.

Explanation: Complexity, if measured either in terms of the number of steps that are needed or along other dimensions, does not necessarily translate to the actions being performed unreliably. The list below represents the characteristics of a complex task or ex-control room task that may be assumed to be performed reliably. If these conditions cannot be established, it is assumed that there are opportunities for error.

In addressing this branch point, the following questions may be helpful[15]:

a) The task does not require skillful coordination of multiple manipulations.
b) The task may be completed at a reasonable pace with ample opportunity for checking instead of having to be done expeditiously.
c) There are no steps that if reversed could cause a failure of the response (e.g., by damaging equipment).
d) There is nothing unusual or inherently difficult about the tasks that would normally cause any problems for those executing the actions.

➔ If any of these statements are not true, take the NO branch; otherwise, if all statements apply, take the YES branch.

It will be expected that, in addressing this question, the analyst will have identified the specific characteristics of the task that create the opportunities for error, and also understand the consequences of the errors. This information will be used later in the assessment of the potential for recovery. There may be more than one opportunity but if they have the same consequence, they may be considered together for recovery.

Branch Point 2: Training

Definition: This branch point is intended to determine whether training is sufficient to minimize the opportunities for error for tasks with some inherently complex aspects.

Explanation: Training is an important factor in ensuring that the responses are carried out correctly. The issue of concern here is whether the crew is well trained on this evolution and that any difficult aspects are addressed clearly and thoroughly during training such that a complex task and/or ex-control room task would be straightforward for trained personnel using procedures.

To address this branch point, the analyst should assess the following:

a) Has the crew been properly trained to understand how the scenario may evolve?
b) Are complex tasks and/or ex-control room tasks covered in training?

➔ If the answer to both is No, take the POOR branch. If Yes to either, take the GOOD branch.

Branch Point 3: Work Practices

Definition: This branch point is intended to determine whether, either as a result of standard work practices or by procedure, there are factors that enhance the likelihood that the task, even though complex, can be performed reliably.

Explanation: There are certain work practices that can be credited with increasing the likelihood that tasks are performed reliably. For example, there could be intermediate checks upon completion of some of the individual steps to confirm that the correct manipulation has been performed.

In addressing this branch point, the following questions may be helpful:

a) Does the procedure include hold points at critical stages to check that, for example, system realignment has been performed correctly?
b) Is it standard work practice for the performer to verify his or her action at each step or another individual is there to check the actions?

[15] Note that these questions are somewhat generic because this tree is intended for any complex task and the detailed nature of the tasks will differ.

➔ Note that these questions should be answered by taking into account the specifics of the task that are conducive to error. If the answer is No to *any* of these questions, take the POOR branch. Otherwise, take the GOOD branch.

Branch Point 4: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.3. The following is additional guidance specific to this CFM. This branch point addresses the possibility that, if the action has not been completed successfully, it may be possible to revisit the response and correct any errors made in the manipulation.

To address the potential for recovery, the first issue is whether there is an immediate indication of the success of the action via a direct measurement of some plant parameter that reflects the success of the function, e.g., water level, pressure (pump flow may not necessarily indicate the water is going to the correct place)? Furthermore, the procedure should require confirmation that the action has been completed successfully. In general this ought to be the case, since there will typically be a step in the procedure to verify that flow has been established. Secondly, it will be necessary to determine that there is enough of a time margin, given the time taken to perform the manipulations in the normal manner, that the failure of the execution could be diagnosed and there is still time to recheck each step to prevent the HFE from occurring. Note that this recovery potential is not intended to apply to control action failures since they are continuous actions and any corrections would be made as part of the evolution.

In addressing this branch point, the following questions may be helpful:

a) Does the procedure allow for an unsuccessful action error to be identified? This is most significant for the case where the indication of success is indirect (e.g., measurement of water level rather than flow).
b) In such a case, does the indication occur in sufficient time to allow the error to be corrected?
c) Does the error identified in the first branch point preclude the possibility of success?

➔ If the answer to *all* of the questions is No, take the NO branch. Otherwise, take the YES branch.

NOTE: This would not apply to control action failures since they are continuous actions and any corrections would be made as part of the evolution (see next section).

5.2.11.3.3.3 Failure to Correctly Execute Response (Control Action)

For this CFM, the crew is performing a prescribed series of manipulations with the intent of achieving some goal such as establishing a pressure or temperature below or above a specified level. This is accomplished by making adjustments and would involve continuous monitoring as the manipulations are being carried out. Failure is difficult to define because there is typically some margin from the optimal response. Since these types of actions, if critical to plant safety, will be trained on and the necessary information should be available to make the relevant adjustments, failure can only occur on gross deviations. One of the factors that could influence this is the plant status, in particular, if there is something about the way the plant is behaving that makes the plant more sensitive to deviations, and if there is a feedback mechanism that guarantees failure. However, this is a system deviation, not a HRA problem.

This could be treated as a special case of the above tree, with a different set of questions about the plant conditions that complicate the task and any conditions that inherently complicate the execution (e.g., control of level in a BWR during ATWS is considered to be challenging).

5.2.12 AP-1: Misread or Skip Step in Procedure

5.2.12.1 Definition of CFM

This CFM deals with slips and lapses in following a procedure. The information in the procedure is clear and unambiguous and the operator/crew simply misreads or skips a step in the procedure. The definition of step is intended to be flexible in that the analyst performing the task analysis of the activities needed for success needs to identify if there is a possibility that the portion of the procedure in effect may either be misread or skipped in such a way that the critical instruction is missed.

Note that there is a separate CFM to cover errors in misinterpreting a procedure. Also, it is not necessary to apply this CFM for the execution phase. The execution CFMs are treated at a fairly high level, and it is not possible to distinguish between skipping a step in the procedure and just failing to perform the action to which it pertained. Finally, while this CFM is a valid failure mode, it should not be expected to be a major contributor to an HFE.

5.2.12.2 Applicability

This CFM is applicable whenever the steps that are missed or misread could lead to an incorrect plant status assessment or a wrong response plan. This CFM is different from other CFMs such as ‘misinterpret procedures’ that covers misreading the procedure due to ambiguous wording or complex logic. Furthermore, this CFM does not cover purposely skipping a step in the procedure. This CFM has a different recovery potential than ‘misinterpret procedures’; it is easier to recover from misreading a procedure than misinterpreting one.

5.2.12.3 Development of Decision Tree

Generally a crew may be led to misread or skip a step in the procedures because of a lapse caused by distraction or forgetfulness. Examples of lapses include instances where operators may forget to perform a specific step, may lose their place in a procedure, or may forget to perform an entire sequence of steps. Lapses most often arise when interrupted in the process of performing a task. The error is, therefore, unintentional and is driven by the workload, procedural complexity and time pressures.

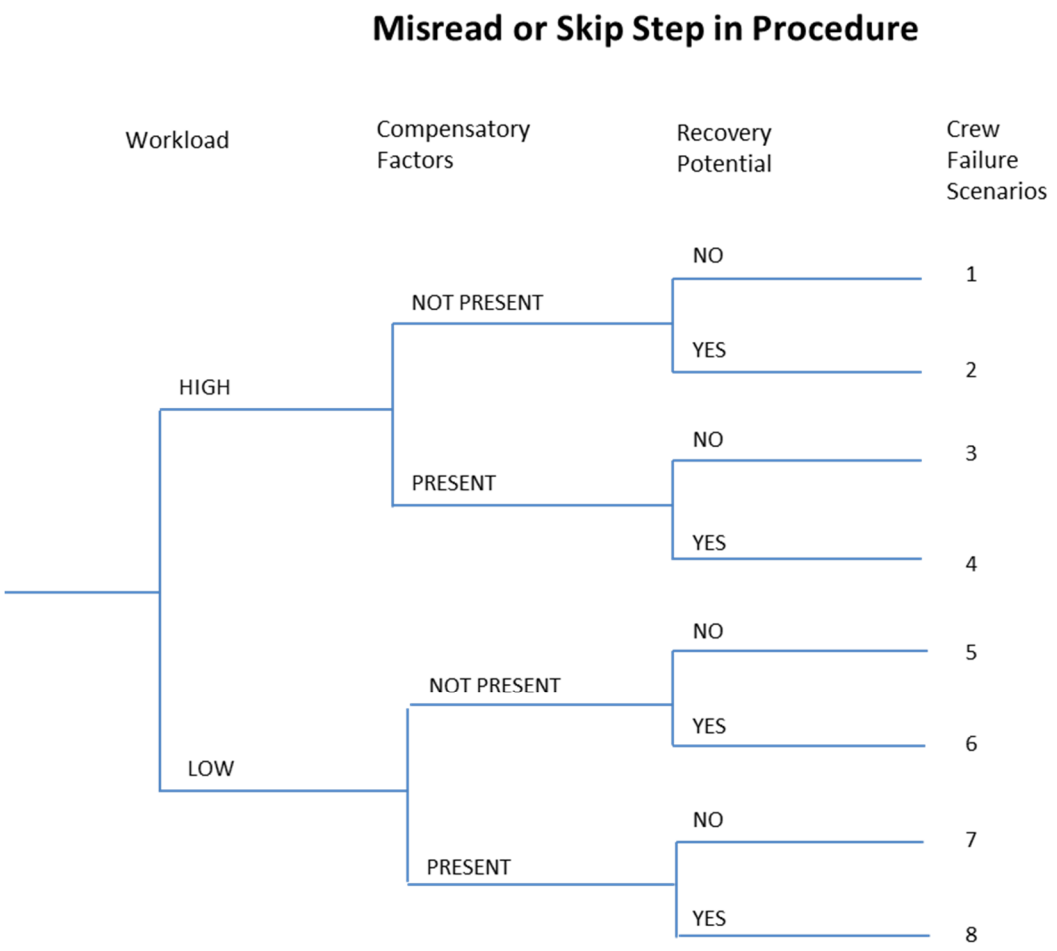


Figure 5-14. Decision Tree for CFM 'Misread or Skip Step in Procedure'

Branch Point 1: Workload

Definition: Workload is considered here as a cognitive workload that can be a source of distraction.

Explanation: Distraction results from a simultaneous demand for attention from other sources (W2, W3), which could result in the crew looking or stepping away from a procedure and picking back up in the wrong place OR could result in the crew misreading the procedure due to interference. The crew may also feel increased workload due to time pressures and the need to accomplish a task immediately (W6).

In addressing this branch point, the following questions may be helpful:

a) Does the need for this response occur when other tasks or procedures are being employed (or the crew needs to respond to several things)? Specifically, is the procedure reader performing other tasks or tracking other procedures (or sections of a procedure) in parallel?
b) Is the accident scenario such that the crew may be interrupted in the middle of their procedure to attend to another task or person?
c) Does this occur when there is a problem or issue that arises that needs to be resolved immediately? Alternatively, is this task one that might be seen as not needing to be attended

to immediately such that another pressing task may take precedence and distract the crew away from the original task?

➔ If *any* of these questions is true, the HIGH branch should be taken. Otherwise, take the LOW branch.

Branch Point 2: Procedure

Definition: This branch is concerned with the way the procedure is structured to determine whether there is anything that might make skipping a step or misreading it more likely.

Explanation: If the procedures are overly complex (e.g., multi-step action, more than one page long, complicated logic), the operator is more likely to make a mistake in reading the procedure or to commit a slip or lapse in following the steps. This complexity does not imply the procedure is poorly written, but only that it is more complicated to understand or follow.

In addressing this branch point, the following questions may be helpful:

a) Are the steps within the procedure clear and have sufficient details for the desired action in the context of the sequence of interest?
b) Are acceptance criteria and tolerances or specific control positions and indicator values properly specified?
c) Are charts, graphs, or figures within the procedure easy to read or understand?

➔ If the analyst answers No to *any* of these questions, the COMPLEX branch should be taken. Otherwise, take the SIMPLE branch.

Branch Point 3: Compensatory Factors

Definition: This branch is concerned largely with work practices that minimize the chance of making the errors of concern.

Explanation: Certain factors may exist that will help to prevent the crew from committing an error in misreading or skipping a step in the procedure. For instance, the crew may make regular use of place-keeping aids which would significantly decrease the opportunity to skip a step within the procedure. Furthermore, if high workload or time pressure is an issue, the crew may have been trained on how to handle the extra pressures.

In addressing this branch point, the following questions may be helpful:

a) Are there work practices in place (e.g., place-keeping aids) that are regularly used by the crew when using the procedures that would prevent misreading or skipping steps?
b) Is the crew trained on how to properly prioritize high workload situations?

➔ If the analyst answers No to either of these questions, the NOT PRESENT branch should be taken. Otherwise, take the PRESENT branch.

Branch Point 4: Recovery Potential

The assessment of whether credit can be taken for recovery is discussed in general terms in Section 5.3. The following is additional guidance specific to this CFM.

Definition: The intent of this branch is to address the possibility that, given the consequence so the error, there is a chance for the crew to recover and avoid failing the function.

Explanation: Misreading or skipping a step in the procedure could be modeled as the operators not performing the required function (error of omission), or as an error of commission (e.g., transfer to incorrect procedure or initiate incorrect response). In either case, what is happening at the plant subsequent to the error has to be understood. The challenge for the analyst is to identify the potential errors that could result from this CFM.

It has to be established that the operators are monitoring the status of the plant and that this behavior is reinforced by their training and/or later procedure steps such that their nonresponse is not appropriate.

Furthermore, the operators must receive feedback from the plant. This feedback would need to be strong enough that it would lead the operators to either revisit the earlier misreading or skipped step within the procedural guidance, consult other procedural guidance that would direct them correctly, or to successfully correct their response in some other manner.

If there is no clear guidance that the operators should do these steps, no recovery should be credited.

5.2.13 C-1: Critical Data Miscommunicated

5.2.13.1 Definition of CFM

This CFM is intended for situations in which critical data is incorrectly transferred between crew members. In this context, data could be an instruction, notification of a parameter value, or a report on the status of a function, system or component. The decision tree for this CFM is not quantified. Instead, the discussion on each of the branch points is intended to help an analyst think through potential conditions that may cause miscommunication. If an analyst feels that miscommunication may be a contributing factor to an HFE, there are a couple of options available for addressing it.

1. Account for the additional burden of communication, and therefore the potential for miscommunication, in the workload or distraction branches of other CFMs. That is, if the analyst feels that miscommunication is a factor, choose the high workload branch.
2. Account for the additional complexity added to completing an ex-control room task due to the need for communications between the control room and the ex-control room location by choosing the “failure to correctly execute response (complex action)” tree.
3. Account for additional miscommunication issues by adjusting the HEP obtained after quantifying through the rest of the decision trees based on the answers to the decision tree presented below. Note that now multiplication factor is offered in this section to account for miscommunication, neither are any estimated HEPs offered for the paths through the decision tree. Therefore, the analyst will need to adjust the HEP obtained from the quantification of the other CFMs based on expert opinion.

5.2.13.2 Applicability

The focus of this CFM is unintentional miscommunication. The failure mechanisms are therefore in the nature of slips rather than a deliberate transference of incorrect data. Failures in intent are captured by the CFMs related to dismissing or discounting data; failures in perception are captured in data misperceived. The intent is to address the PIFs that can impede successful communication.

This is applicable when the performance of the task involves transference of information between crew members. The failure scenarios that result from this CFM tree include both the failure that results in directing a crew member to obtain incorrect information (e.g., data from the wrong train), and the transference of the incorrect data to the procedure reader and decision-maker. A third instance could occur in which the correct data is communicated, but it is not heard due to either distractions or other environmental factors (e.g., high noise). In this context, data could in fact be an instruction rather than a parameter value.

It should be noted that the inclusion of this CFM is an approximation that is in lieu of developing an interactive crew model.

5.2.13.3 Development of Decision Tree

In developing this decision tree, attention is given to communication. Communication is essential to all but the simplest tasks performed by the crew. Furthermore, some tasks may require significant continuous communication. Finally, simpler tasks may require the communication of a single datum or a simple instruction. For all of these cases, the first consideration should be to discriminate those cases where communication is complex and those where it is simple. One way of addressing this is through workload. If the workload is high due to competing coincident tasks or because the task itself is complex, the chance of miscommunication is increased.

In either case, environmental or other factors that hinder communication should be addressed. This is more of a concern for ex-control room actions than it is for in-control room actions.

The use of a well understood protocol for communication can serve to reduce the possibility of miscommunication. This reduces the risk of mishearing but does not prevent an incorrectly perceived piece of data being transmitted. Mishearing is a possible failure for this CFM, whereas misperception is dealt with in another CFM.

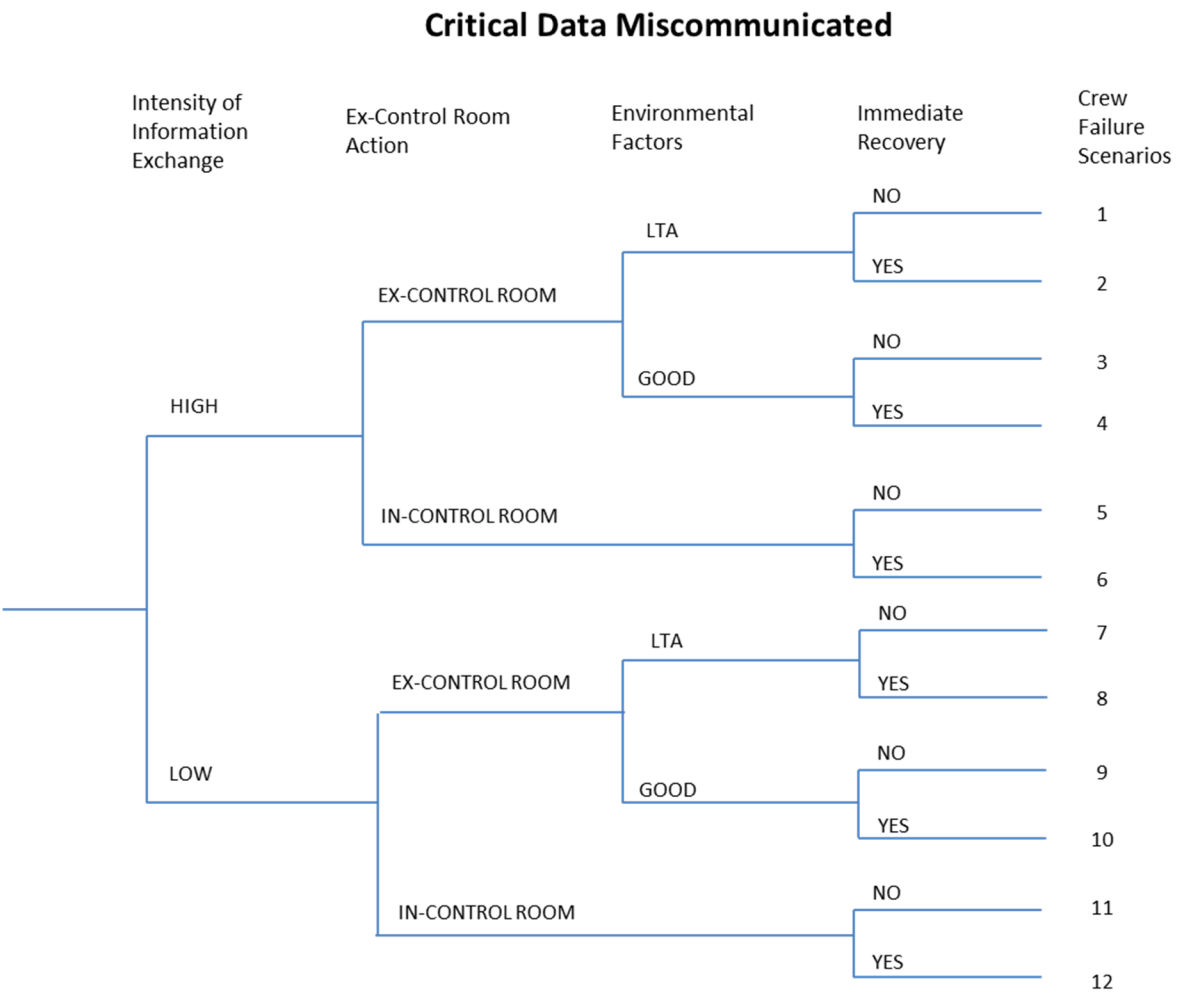


Figure 5-15. Decision Tree for CFM 'Critical Data Miscommunicated'

Branch Point 1: Intensity of Information Exchange

Recognizing that communication is an ongoing activity, this branch point distinguishes between the normal (characterized as low) intensity of communication for which operators are well trained and are capable of maintaining, and those cases where it is abnormally cognitively demanding. In this context, therefore, intensity of information exchange is a surrogate term for cognitive workload, which, if abnormally high, could be a source of distraction or otherwise inhibit the ability to communicate in an accurate manner, such that there is an increased likelihood that the source does not transmit a critical request or piece of data, or that the target does not register it. This distraction could come from the speaker (either the source or the target) attempting to complete multiple tasks (e.g., collecting multiple pieces of information for a single complex task, or keeping track of a number of functions) simultaneously.

Intensity is high if the communication is required at a time of high activity or if the task itself is abnormally complex[16] and requires frequent exchange of information. High activity may be for the source or the target operator such as one or the other must attend to multiple sources of information (including other operators), alarms or tasks, or they must keep track of more than one function simultaneously.

Another option for dealing with this element of miscommunication is to account for it in other CFMs as high workload. Specifically, the CFMs of 'data misleading or not available' or 'wrong data source attended to' may be relevant.

In addressing this branch point, the following questions may be helpful:

a) Does the miscommunication occur at a time when the source or target operator must attend to multiple sources of information (including other operators), alarms or tasks?
b) Does the miscommunication occur at a time when the source or target operator must perform more than one task at once?
c) Does the miscommunication occur at a time when the source or target operator must keep track of more than one function simultaneously?

➔ If any of these is true, take the HIGH branch. Otherwise, take the LOW branch.

Branch Point 2: Ex-Control Room Action

This branch differentiates between those crew responses that can be accomplished entirely within the control room, and those where some of the essential activity takes place outside the control room and where remote communication is necessary. The remote communication could be related to the collection of information to assess the plant status or for manipulation of equipment. For the latter, if, as is sometimes the case, the operator does not need to communicate with the control room while performing the task (e.g., if he has the written instructions with him), this CFM would not apply. The assumption is that for an in-control room activity, there are essentially no impediments to communication, since that is the "normal" environment. There is expected to be a differentiation between the HEPs for the complex and non-complex cases which would account for the potential distraction caused by an increased number of alarms, etc., in the former case over the latter. There's really no need to be concerned about issues like smoke in the control room since, if it is assumed that this is a boundary condition for the response, control room abandonment would be assumed to occur.

The direction taken by this branch point is entirely driven by the accident scenario and knowledge of the required response.

[16] Complexity in this sense is related to an abnormally high cognitive load.

If this factor is found to be the only relevant driving factor to the potential for miscommunication, then it is best dealt with by using the CFM and decision tree for 'failure to correctly execute response (complex action)'. If remote communication is necessary, then the complex action tree should be chosen over the simple action tree.

The answer to the following question should be determined:

a) Is an operator in the control room required to communicate with someone outside of the control room (i.e., the communication does not solely occur inside of the control room)?

➔ If the answer to this question is Yes, take the EX-CONTROL ROOM path. Otherwise, take the IN-CONTROL ROOM path.

Branch Point 3: Environmental Factors

This branch captures factors that can hinder communication. Environmental issues include excess noise – this may be especially true in an ex-control room location in which excess noise may degrade the quality, clarity or volume of the message. Environmental issues may also include factors (e.g., steam, temperature) that might affect the ability of the operator to correctly obtain the required information.

In addressing this branch point, the following questions may be helpful:

a) Is the required equipment (telephone, walkie-talkie, etc.) unavailable or degraded to the point that the message becomes ambiguous or interferes with communication (e.g., SCBAs)?
b) Is there excess noise in the local, ex-control room environment that degrades the quality, clarity or volume of the message?
c) Are there environmental factors (e.g., steam, temperature) that affect the ability of the operator to correctly obtain the required information?

➔ If the answer is Yes to any of these questions, the LTA ('less than adequate') path should be taken. Otherwise, take the GOOD path.

Branch Point 4: Immediate Recovery

This branch addresses immediate recovery, and factors include a third party checker, which will be dependent on the scenario and the ability of the checker to be effective. It may be less relevant for the high intensity in-control room cases than for the low-intensity cases.

5.3 Treatment of Recovery

In general, there are three categories of recovery for a given HFE:

1. Immediate recovery: this is a usually a recovery that is applied to slip-type errors (i.e., crew has correct mental model and response strategy) that are noticed either by the operator himself (self-review) or by a crew member (e.g., peer check). This is most applicable when the incorrect action or omission of the action provides an immediate cue that something is wrong (e.g., plant doesn't respond as expected). In IDHEAS, there is not usually a specific recovery credit applied for this type of recovery, however, some level of self-review/peer-check is credited in the development of the HEPs for each DT; that credit is reduced for branches where there is high workload/distraction. For execution CFMs, immediate recovery via verification steps and other factors is explicitly evaluated as part of the "Work Practices" branch. Similarly, for the Miscommunication CFM, immediate recovery is explicitly evaluated as part of the DT.
2. New Cue Prompts Recovery: this recovery is an additional cue (procedural or alarm) that presents new information and forces the crew to reevaluate their current path. The nature of the cue must be strong enough to put the crew back on a success path, and there must be sufficient time to get to new cue and perform the correct action. This type of recovery is

addressed explicitly in the DT ("Recovery Potential" branch point) for the relevant CFMs. This recovery is discussed further in the reminder of this section.

3. Long Term Recovery: Some actions have very long time frames that allow for an independent review of the overall strategy (e.g., shift change, review of TSC/ERF, etc.). This type of recovery is not explicitly credited in IDHEAS, but when appropriate, the analyst may choose to credit this type of recovery when a strong case can be made for its efficacy. No guidance is currently provided on the level of credit that can be given for this type of recovery.

The following table provides a tally of CFMs which include a branch point labeled recovery or recovery potential.[17] The remainder of this section provides general guidance on how to assess whether or not credit can be given for recovery under this branch point. Additional, CFM-specific, factors to consider when crediting recovery are provided in the DT guidance for each CFM. It is expected that to credit recovery for a given CFM, the strength of the recovery cue must be commensurate with the type of error (e.g., misperception errors are easier to recover from than errors that result in an incorrect mental model).

[17] The method for addressing recovery presented here is to include it as an integral part of the decision tree structure, and essentially deal with recovery based on an assessment of the opportunities identified in the CRT and whether they are relevant to the CFM. Other, more explicit approaches will be explored to determine if they bring additional insights.

Table 5-2. CFMs with recovery potential branch points

CFM	Recovery Potential Branch Point?	Comment
AP-1 Misread or Skip Steps in Procedures	X	
AR Key Alarm no attended to		Boundary condition for this CFM is that the alarm is the only cue for action, so, by definition, there is no recovery potential.
SA-1 Data Misleading or not available		Boundary condition for this CFM is that remaining on a success path hinges on understanding the plant status in spite of the misleading or unavailable indication. The DT deals explicitly with factors that would allow the crew to understand the plant status given the state of the indication (e.g., this whole CFM is really a recovery for the misleading indication).
SA-2 Wrong Data Source Attended to	X	
SA-3 Critical Data Incorrectly Processed/Misperceived	X	
SA-4 Critical Data Dismissed/Discounted	X	
SA-5 Premature Termination of Critical Data Collection	X	
RP-1 Misinterpret Procedures		
RP-2 Choose Inappropriate Strategy	X	
E-1 Delay Implementation	X	This CFM is applicable to deciding to delay a step which the crew has already received a procedural cue to perform and the crew knows that the action needs to be done. Therefore, an alarm, if available, can be credited to bring the operator's awareness back to the urgency of that action.
E-2 Critical Data not Checked/Monitored with Appropriate Frequency	X	Monitor task, so an alarm, if available, can be credited for recovery.
E-3 Fail to Initiate Execution	X	
E-4 Fail to Execute Simple Response Correctly	X	
E-5 Fail to Execute Complex Response Correctly	X	

In this context, the inclusion of the recovery branch is a reflection of the possibility that the initial fault on the part of the crew, as expressed by the CFM, may be corrected before the failure represented by the HFE occurs. It is assumed that the crew acts in accordance with the failure mode, e.g., if they have dismissed or discounted a piece of critical data, they act on the basis of the plant status consistent with that error. Recovery is possible if, before the plant status evolves to the state where no correction is possible, the crew is able to recognize that their response is not working and are able to do a mid-course correction. That recovery is possible at all is a result of the fact that there is typically a time window for successful completion of the required response, and that failure of the associated function does not occur directly upon the initial failure by the crew. For the CFMs not included above such a recovery is not credited. For example, the CFM 'delay implementation' is defined in such a way that functional failure occurs directly as a result of the delay.

This type of recovery is distinguished from the positive PIFs that are included in some of the branches of the decision trees. Examples include the skill-of-the-craft implementation of searching for confirmatory indications and the existence of an alarm that is directly related to the required response. These positive attributes prevent the failure from occurring in the first place, whereas the recovery branch is a correction of a failure that has occurred. This branch addresses the possibility that new information comes into play once the crew has deviated from the required response.

To address recovery for this cause-based model, an assumption is made that the crew is operating using a mental model of the plant status and its expected evolution. Therefore, recovery can be thought of as a sort of Bayesian process in which the crew gains new information and updates its mental model. A high likelihood of recovery would generally be associated with scenario evolutions whose characteristics include:

- The plant status evolution, as determined by parameters monitored by the crew subsequent to the error, should be sufficiently at odds with the mental picture of the plant such that it can create a need to reassess the response. In other words, the new evidence is strong.
- The newly revealed plant status is such that there is a plan or procedural path for correct response given a revised mental model.
- The arrival of the new information and its assimilation can happen in sufficient time to allow the correct response to be effective and prevent the HFE.

Therefore, to determine whether to take any credit for recovery, the analyst must develop an understanding of the evolution of the plant status including the timing of any relevant cues and the expected crew activities (including their path through the procedures), following the initial incorrect response (as characterized by the descriptor for the CFMs). This is an activity that is carried out in order to construct the CRT, and the significant opportunities for recovery should be represented on the CRT as branch points off the path representing the failure to perform a critical task. For some cases, the identification of a recovery opportunity is quite simple. For example, in both Westinghouse and B&W procedures, if the crew member following the EOPs does not realize the need to begin feed and bleed, the crew member tracking the critical safety functions with his or her own procedure can identify the need. However, some of the more complex recovery opportunities, particularly from errors of commission, may be more difficult to identify.

The likelihood of recovery will depend on the nature of the CFM. For example, in the case of execution errors, the mental model may be correct, and therefore, if the plant response is not as expected, the source of the error may be easier to detect by checking the status of the equipment that has been manipulated. If however, the error is one of having developed an incorrect mental model of the plant status, the new evidence has to be such that it is not possible to invent a reason why the plant is behaving the way it is and still be consistent with that mental model.

In order to justify taking credit for recovery, the analyst should determine:

- How the plant status is changing following the error.
- What path through the procedures the crew is following, what new information will be revealed, and what does the procedure indicate about the plant status given this information.
- Whether and how the crew monitors the status of the plant to determine if the plant response is as expected (e.g., if they think they are adding inventory do they check that level is stabilizing or increasing?) This may be a parallel activity to the above.
- Establish the time line for the new information and the necessary corrective responses to determine if this can be achieved given the success criterion for the response.

Up to this point, given that opportunities have been identified and the time available has been assessed and found adequate, it can be determined that recovery is feasible. The assessment of whether success is likely is somewhat more subjective. The factors that enter into this assessment include:

- How the crew interacts; who's doing what and with what resources (e.g., what procedures and displays they are using).
- What is the standard practice when the plant response is not as expected with respect to checking system alignments, etc. (particularly significant for execution errors)
- How the training plays into the processing of this new information. This should address the significance given to the information that could change the mental model. What is the practice given to the resolution of information that conflicts with expectations? Is the latest information given more credence or treated with more urgency?
- Is there likely to be reluctance to follow any procedural guidance associated with the newly acquired information on plant status?

Answering these questions requires significant judgment on the part of the analyst, and requires interaction with knowledgeable plant staff. If a convincing case cannot be made, no recovery should be assumed.

5.4 References

1. Whaley, A. M., Xing, J.,Boring, R. L., Hendrickson, S. M. L., Joe, J. C., LeBlanc, K. L., & Lois, E. (in publication). Building a Psychological Foundation for Human Reliability Analysis. (NUREG-2114, INL/EXT-11-23898). Washington, D.C.: U.S. Nuclera Regulatory Commission.
2. Nuclear Regulatory Commission (NRC) (2000). Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA). (NUREG-1624, Rev. 1). Washington, DC: U.S. Nuclear Regulatory Commission.
3. 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.
4. Swain, A. D. & Guttmann, H. E. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. (NUREG/CR-1278; SAND80-0200). Washington, DC: US Nuclear Regulatory Commission.
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 IMPLEMENTATION OF THE IDHEAS METHOD – HEP ESTIMATION

6.1 Introduction

In this chapter, we describe how the quantification model presented in Chapter 5 is used in conjunction with the CRD developed in Chapter 4 to estimate the probability of an HFE. To recap, an HFE is defined as part of a PRA scenario. It is defined as a failure of operators to perform a required function in response to the particular plant status, i.e., operability status of systems or functions following an initiating event. The detailed definition includes a specification of the success criterion(a) for the key safety function(s) challenged in terms of the required operator response at a functional level and the time window by which the response has to be completed to achieve success and prevent the failure. In addition, the definition includes an identification of the existence and timing of the cues or other indicators the crew may use and the procedure or other guidance in effect.

As described in general terms in Chapter 2, the IDHEAS process begins with this definition of an HFE, and following an assessment of the feasibility of the response, qualitative analysis is performed to develop a detailed understanding of the critical tasks and associated cognitive and execution activities needed for success as a prerequisite for identification of opportunities for failure. This involves constructing a timeline, based on the representative PRA scenario to find out what and when the information the crew needs to formulate its response (whether it be procedure guided or experience/training/skill of the craft based) becomes apparent, and when the crew is in a position to use that information to execute the required response. Furthermore, this analysis identifies the opportunities the operating crew has to correct an error they may have made (e.g., taking an incorrect path through the procedures) in time to prevent failure of the function. This is the basis for the CRD, and is described in detail in Chapter 4.

The second major element of the IDHEAS process (after developing the CRD) is the quantification model presented in Chapter 5. Section 6.2 describes how the quantification model is applied to the results of the task analysis as represented by a CRD, and specifically addresses the identification of the relevant CFMs for each of the crew failure paths represented on the CRD, the estimation of the probability of each applicable CFM for each failure path, and the calculation of the HEP for the HFE. This chapter therefore describes the implementation of these aspects of the IDHEAS process.

To illustrate the quantification process, the example analysis started in Chapter 4 is continued here in Section 6.3. Appendix A also contains three examples of the application of the IDHEAS process.

6.2 Implementation of the Quantification Model

The overall process flow of quantifying an HFE described in this chapter is illustrated in Figure 6-1. The input to the quantification process is the outcomes of different qualitative analyses, and the output of the process is the HEP estimated for the HFE. The process includes the following major steps:

- Step 1: Preparation (Entry condition): Organize the qualitative analyses associated with characterizing the failure paths on the CRD.
- Step 2: Select CFMs applicable to the failure paths on the CRD, based on the definition of the nodes in terms of the critical tasks and specific activities needed to complete the response.
- Step 3: For each CFM, determine the DT path using the DT branch questions.
- Step 4: Calculate the HEP for the HFE.

The implementation of these steps will be described next. We only describe the high-level process of these steps. Detailed implementations need to refer to the descriptions in previous chapters as indicated, and are elaborated on in the examples in Section 6.3 and in Appendix A.

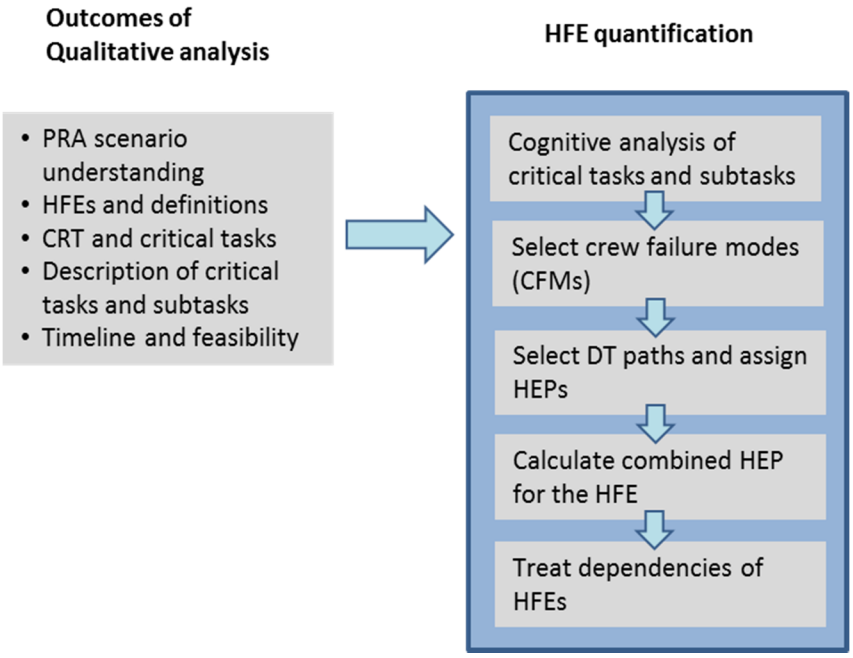


Figure 6-1. Diagram of the quantification process

6.2.1 Step 1: Organize the qualitative analyses associated with characterizing the failure paths on the CRD

The necessary inputs for HFE estimation include the following:

1. Definition of the HFE – PRA scenario context
2. CRD failure paths for the HFE, including definition of response nodes in terms of the critical tasks and the associated activities required for success
3. Timeline and demonstration of feasibility.

The definition of the HFE as determined by the PRA model is discussed in Chapter 2, the process of performing the qualitative analysis for 2) and 3) is described in Chapter 4, and the feasibility assessment is described in Chapter 3. In this section, we recapture the main outcomes of the analysis and describe their use in the quantification model.

6.2.1.1 Definition of the HFE

The definition of the HFE includes operator action success criteria, relevant procedural guidance, cues and indications, available time, and high-level tasks required to achieve the goal of the response. These outputs serve as the input to other aspects of the qualitative analysis. In addition, they provide an overall understanding of the context of the HFE, and such an understanding is used to build a baseline mental model of the HFE for analysts to perform HFE quantification.

6.2.1.2 CRD Sequences for Quantification

The CRD is described in Chapter 4. The outcome of the CRD task representation and selection is a set of nodes and associated critical tasks and activities that, if not performed correctly,

would lead to the HFE. The HEPs of these critical activities will be estimated for calculating the overall HEP for the HFE. In addition, while developing the CRD, a timeline has been developed.

The nodes corresponding to the branches along the top of the CRD represent critical transitions in the guidance that, if not followed correctly, would lead to the HFE. While it is possible to represent each individual critical step of a procedure that constitutes a critical task or activity as a branch in the CRD, some agglomeration may be desirable for ease of communication. In its compact form presented in Chapter 4, the nodes of a CRD represent a failure to make an appropriate transition to or within a procedure, or a failure to initiate a response or perform the response correctly, each of which can be characterized as a high level critical step. As discussed in Chapter 4, success at each node is characterized as requiring success in one or more critical tasks each of which involves a number of cognitive and execution activities. For example, transitioning to the correct procedure could involve obtaining specific pieces of information and using a criterion to determine the transition. Once a CRD node is defined in terms of one or more critical tasks and associated activities, the relevant CFMs need to be identified. The HEPs for each relevant CFM are combined to obtain the HEP for the CRD path.

Secondary branches, i.e., those branches on the failure branch of one of the nodes described above (see Figure 4.3 in Chapter 4), represent opportunities to recover from the prior mistake. The information needed to address these should have been developed as result of the investigation of the failure time line (e.g., the occurrence of any cues that would facilitate recovery to the success path, and the procedural guidance to perform the appropriate response). However, these nodes are not decomposed in the same way as the primary nodes. The opportunity for recovery is assessed on CFM specific basis and included in the choice of path through the associated decision tree.

In any case, the end result of the qualitative analysis up to this point is a clear definition of what tasks and activities are required for success at each branch of the CRD. Given this, and an understanding of the cognitive requirements for each of the tasks, the analyst can screen which of the CFMs are relevant for each task. Note that a CRD developed to a greater level of detail would not necessarily lead to a greater number of CFMs being relevant for any individual HFE since the CFMs apply to different stages of information processing. For example, if instead of modeling a branch as “determine that the level is less than some criterion” with all that entails (getting the data, assessing it correctly, doing the right comparison with the procedure) implicit in that branch, the analyst chooses to model the act of obtaining the data associated with the level as a separate branch from the comparison with the criterion, the number of applicable CFMs in total would not change, since those CFMs associated with data collection and perception would only apply to the former branch and would not appear in the latter.

6.2.1.3 Timeline

The timeline represents the occurrence of events related to the crew’s critical tasks in responding to an event and can also include necessary non-critical tasks (e.g., communicating with entities outside the control room) along the timeline. While precise timing of individual tasks is not required, it is important to identify the ordering of critical events, e.g., when does a plant parameter reach a critical value that triggers a response, and when does the operating crew reach the step in the procedure that addresses that critical value? Furthermore, the estimates of the time have to be realistic enough to allow a determination of whether the response is indeed feasible.

For each failure of a critical task on the CRD a separate time-line is developed to determine the feasibility of the potential recovery path when applicable given that the time required for recovery may reduce the time available for other needed actions.

6.2.2 Step 2: Selection of CFMs for Each CRD Failure Path

A prerequisite for performing this step is the characterization of the critical tasks in terms of the specific activities identified as essential for success at the nodes of the CRD and their cognitive requirements, since this will be used to identify the relevant CFMs. This can be characterized as a cognitive task analysis, but also includes addressing the execution portion of the operating crews' response.

The outcomes of cognitive task analysis, along with other outputs of the qualitative analysis, provide the structured context for the HFE and critical tasks and tasks.

For each of the branches coming from the top line of the CRD, the analyst identifies, from a description of the critical tasks and activities needed for success captured in the branch, the relevant CFMs. This is done prior to assessing the PIF characteristics in the DTs to come up with the HEP contribution. The branches developed along the down path represent opportunities for recovery and these are also addressed in the decision trees (i.e., the potential for recovery of most of the CFMs is addressed within branches of the DTs themselves).

The rationale for identifying potentially relevant CFMs is captured in the Table 6-1. The first column of the table describes the response phase for which the CFM could be relevant. Only those response phases involved in the critical task need be addressed. So for example, if the critical task being evaluated does not involve execution, then none of the execution CFMs would apply. Then for each response phase, if the answer to the question in the second column is yes for the task or activity being evaluated, the DT for that CFM may be used to evaluate the probability of that CFM. Those for which the answer is no are screened from consideration because the CFMs are not applicable.

Table 6-1. Rationale for identification of potential CFMs

Response Phase	CFMs	Guidance
All Phases	AP-1: Key Alarm Not Attended To	Does success require alarm response?
	AP-2: Misread or Skip Critical Step(s) in Procedure	Is a written procedure being used?
Status Assessment	SA-1: Data Misleading or not Available	Does success require data collection to assess plant status?
	SA-2: Wrong Data Source Attended To	
	SA-3: Critical Data Misperceived	
	SA-4: Critical Data Dismissed/Discounted	
	SA-5: Premature Termination of Critical Data Collection	Does success require monitoring a critical plant parameter?
Response Planning	RP-1: Misinterpret Procedures	Does the success require a decision (e.g., transfer to another procedure, or initiate action)?
	RP-2: Choose Inappropriate Strategy	Does the procedure allow a choice of strategies?
Execution	E-1: Delay Implementation	Does success require responding when a critical value is reached (given the value has been recognized)?
	E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	Does success require monitoring for a critical plant parameter as a cue to initiate response?
	E-3: Fail to Initiate Execution	Does the task require action on plant systems?
	E-4: Fail to Correctly Execute Response (Simple Task)	
	E-5: Fail to Correctly Execute Response (Complex Task)	

6.2.3 Selection of Path through the Decision Trees and Assignment of HEPs

The selection of the path through the decision tree (DT) for each CFM is determined based on completing the qualitative analysis needed to answer the questions associated with the branch points in the DT, taking into account the context determined by the HFE definition. Each of the paths through a decision tree represents what is called a crew failure scenario. Therefore, the end result of this part of the analysis is the identification of the set of crew failure scenarios (one for each relevant CFM) that contribute to the HFE. For each crew failure scenario, the contribution to the HEP is that associated with the path through the DT.

6.2.4 Calculation of the HEP for the HFE

In the quantification approach using the equation below and the current form of the DTs, the CRD is not interpreted as an event tree to be quantified with split fractions, but as an aid to the qualitative analysis to identify the crew failure paths, and as an aid to quantification that can be used to identify the relevant CFMs and crew failure scenarios for the HFE. The DTs are constructed to specifically address recovery where applicable and in this way are able to deal directly with the dependency between the mode of failure and the potential for recovery. Therefore, the HEPs derived from the DTs are used to quantify the complete crew failure path beginning with the initial departure from the success path and the failure to recover. In other words, the conditions for recovery are examined relative to each relevant CFM and the appropriate path through the DT is selected. When recovery is feasible, the recovery possible branch is taken on the DT and the HEP accounts for the failure to recover. If no recovery is feasible, the NO branch is taken and the HEP is correspondingly higher.

Then the overall HEP for the HFE is evaluated by summing the probability of failure from each of the critical tasks or activities (and corresponding CFMs) identified in the CRD (either as nodes or within the definition of a node), and as discussed above, the probability of failure for each task or activity accounts for the potential for recovery from a failure to perform that task or activity. The probability of failure from a key task activity is the sum of the failures from the applicable CFMs for that task or activity. Thus, the quantification of the HEP for the HFE takes the following form for a PRA scenario S:

$$HEP(HFE|S) = \sum_{CRD\ sequence} \sum_{CFM} Prob(CFM\ |CRD\ sequence, S) \qquad \text{(equation 3)}$$

where the outer sum is over the CRD sequences that leads to the HFE, and the inner sum is over the CFMs that are relevant for the CRD sequence. The term $Prob(CFM\ |CRD\ sequence, S)$ is the probability associated with the end point of the path through the DT for the specific CFM that is determined by the assessment of the relevant contextual factors associated with the HFE (and the CRD sequence). These contextual factors are determined by answering the questions associated with the branches on the DTs, given the information from the qualitative analysis associated with defining the HFE.

Because the probabilities associated with the end points of the paths through the decision trees are predefined, when analyst to analyst differences arise, they would primarily derive from the assessment of the PIF characteristics. For this reason, the documentation associated with the derivation of the CRD and the assessment of the choice of CFMs and the contextual factors (PIFs) is a crucial part of the HRA task.

Note that equation 3 is written symbolically as the rare event approximation. When the individual contributors to the equation i.e., when some of the individual terms $\boldsymbol{Prob(CFM\ |CRD\ sequence, S)}$ are large, e.g., on the order of .1, the equation should be solved taking into account that this is a probabilistic sum. For example if there were only two contributors A and B, then the correct sum would be: $(HFE) = Prob(A) + Prob(B) - Prob(A) * Prob(B)$.

6.2.4.1 A Special Case

The above formulation assumes a linear relationship between the critical task and the CFMs. In other words the critical tasks can be described as consisting of a linear series of activities. However, for some critical tasks, this is not the case. An example is plant status assessment task that requires determining the status of several plant parameters, each of which has the same cognitive requirements. If a decision is made on the basis that more than one of the parameters is outside a specified range, this represents an AND logic, where failure occurs if all the relevant parameters are incorrectly processed. If, using the DTs for each of the potentially applicable CFMs for each of the parameters results in a low HEP, the analyst may argue that the likelihood of all the parameters being incorrectly processed is sufficiently small that the contribution to the overall HEP can be screened out. The argument may be stronger if the parameter ranges of concern would likely be correlated in some way, e.g., if a (unfavourable) high pressure is always associated with a (unfavourable) low level.

6.3 Example Quantification of an HFE

The example analysis of an HFE representing the failure to initiate feed and bleed (F&B) in a total LOFW scenario is continued in this section. Section 4.4 presented the task analysis for this HFE, including the CRD and the documentation of its nodes. Further examples are provided in Appendix A.

6.3.1 Inputs to Quantification –HFE Definition and Task Analysis

The outputs of the qualitative analysis are listed in Table 6-2, with references to the information documented for the HFE in this example. This information was collected during the development of the CRD for the HFE and organized by referencing the nodes for the critical tasks and the nodes for the error correction opportunities.

To implement equation 3, the first step is to characterize the CRD sequences that have been developed as crew failure paths for the HFE. Each crew failure path corresponds to the failure of a critical task on the expected success path, in this case, the tasks corresponding to Nodes 4, 5, and 6. A discussion of these failure paths is summarized in Table 6-3. The tasks for these critical tasks are listed in the middle column – they are characterized in terms of the nature of the task and the relevant procedural guidance and information available from the plant, as can be seen in Section 4.4.3.1 for Node 4. The error correction potential for each crew failure path or failure of a critical path is listed in the right column; it can be seen that the error correction potential is specific to the critical task.

The next step is the identification of the CFMs applicable to each of the crew failure paths, as presented next (Section 6.3.2).

Table 6-2. Outputs of the qualitative analysis for the example HFE

Outputs of the qualitative analysis	Documentation of the qualitative analysis for the example
PRA scenario understanding	The PRA scenario consists of the initiating event, the subsequent hardware and operator action events leading up to the demand for the operator action, and the success criteria. This information is summarized in the HFE definition provided in Section 4.4.1. The scenario is elaborated in more detail in the CRD and the supporting documentation. The overall CRD and the documentation of all nodes then integrate the understanding of the PRA scenario as a plant evolution and the associated crew response on the expected success path.
HFE definition	Section 4.4.1
CRD: success path, critical tasks, error correction potential	The complete CRD is shown in Figure 4-6. The expected success path is the sequence from node 1 to node 6. Nodes 1-3 describe the scenario from the initiating event, setting up the context for the operator action; they are described in 4.4.2.1-4.4.2.3. The critical tasks are identified with nodes 4, 5, and 6. Node 4, “Enter FR-H1” Node 5, “Decision to initiate F&B and transfer to FR-H1 Step 10” Node 6, “Implement F&B per FR-H1 Steps 10-13” In this scenario, three crew failure paths are identified; these correspond to the failures of nodes 4, 5, and 6, respectively. The error correction potential is represented in the CRD as Nodes 7, 8, and 9.
Description of critical tasks, tasks or activities	The critical tasks are delineated and described in Stage 1 of the qualitative analysis. This corresponds to the information provided in Sections 4.4.2.4-4.4.2.6. Stage 2 of the qualitative analysis extends the description of the critical tasks by decomposing these into critical activities. The latter are documented in Sections 4.4.3.1-4.4.3.3. Stage 3 of the qualitative analysis documents the error correction potential represented by nodes 7-9. These are documented in Sections 4.4.4.1-4.4.4.3.
Timeline	Table 4-3.

Table 6-3. Crew failure paths for the example HFE, critical tasks and tasks

Crew failure path	Critical tasks	Error correction potential
Crew failure path #1 failure of Node 4, "Enter FR-H1" (critical task)	Monitor CSFST for Heat Sink, which involves two tasks (Note 1): Task 1: Monitoring the CSF Status Tree for Heat Sink Criterion 1 "NR Level… Task 2: Monitoring the CSF Status Tree for Heat Sink Criterion 2 "Total AFW Flow… Section 4.4.3.1 NOTE: Both these criteria need to be met to transfer to the RED path, and therefore these are considered to be critical tasks.	Node 7: Periodic monitoring of CSFST for heat sink by STA Section 4.4.4.1 NOTE: Since the monitoring is performed by the same crew member the case for recovery will not be strong.
Crew failure path #2 failure of Node 5, "Decision to initiate F&B and transfer to FR-H1 Step 10" (critical task)	Evaluate the criteria listed in FR-H1 Step 2, entitled "Check secondary heat sink" and go to FR-H1 Step 10 Section 4.4.3.2 NOTE: While other tasks were identified in the qualitative analysis (e.g., trip RCPs) they are not considered critical to success and are not analyzed.	Node 8: Application of the FR-H1 Conditional Information page, first condition "RCS B&F Criteria After Step 1" Section 4.4.4.2
Crew failure path #3 – failure of Node 6, "Implement F&B per FR-H1 Steps 10-13" (critical task)	The critical task consists of executing the following procedural steps: Step 10 (of FR-H1). Actuate SI Step 11. Verify RCS Feed path Step 12. Establish RCS Bleed path Step 13. Verify Adequate RCS Bleed Path Section 4.4.3.3 NOTE: While each step in the execution can be interpreted as a separate tasks, in IDHEAS, these execution steps will be analyzed in an integral manner. Steps 10 and 12 are the critical manipulations. The verification steps provide opportunities for recovery.	Node 9: The feed path and the bleed path are each verified in Steps 11 and 13. Note that successful performance of Steps 10 and 12 (within the time window) satisfies the HFE success criteria. Section 4.4.4.3

Note 1: This is a case where both parameters have to be assessed correctly for the correct transition. Therefore an error in either of these (OR logic) would result in failure. It is for this reason they are referred to as tasks, and should both be taken into account when assessing the HEP.

6.3.2 Identification of the CFMs Applicable to the HFE

This section presents the identification of the CFMs applicable for the crew failure path #1, in which the critical task represented by CRD Node 4 is not performed correctly. It concludes with a listing of the CFMs identified as applicable for all three crew failure paths for this HFE.

The definitions of the CFMs in Chapter 5 and Table 6-1, "Rationale for identification of potential CFMs", which identifies key characteristics of the critical task with questions about the nature of the critical tasks, are used to select the applicable CFMs. The rationale for screening out a CFM (marked as not applicable or n/a) or identifying a CFM as applicable is shown in Table 6-4 for Task 1 of Node 4 (the critical task for crew failure path #1).

The result is shown in Table 6-5, where only the applicable CFMs are shown, together with the associated rationale. The rationale highlights the information from the qualitative analysis that is used. During the quantification, both the questions concerning the applicability of the CFM and the subsequent DT branch (header) questions may lead the analysts to obtain additional information and or clarify the information presented in the qualitative analysis.

Table 6-4. CFMs identified as applicable for critical task Node 4, Task 1

Crew failure path	Tasks or activities	CFM	Applicability and rationale
Crew failure path #1 failure of Node 4, "Enter FR-H1" (critical task)	Task 1: Monitoring the CSF Status Tree for Heat Sink Criterion 1 "NR Level… Section 4.4.3.1	AR: Key Alarm not Attended to	n/a – An alarm is not involved.
		SA-1: Data Misleading or not Available	n/a – The SG level indications are trending down since the start of the transient and reactor trip. All indications are appropriate for this scenario. See Example A1 for where this is not the case.
		SA-2: Wrong Data Source Attended to	**SA-2 is potentially applicable.** WR levels could potentially be attended to instead of NR levels. They will indicate larger percentage values.
		SA-3: Critical Data Incorrectly Processed/Misperceived	**SA-3 is potentially applicable.** The level value expressed as a percentage may be misperceived.
		SA-4: Critical Data Dismissed/Discounted	n/a – The level criterion is below what could be expected in a normal reactor trip situation.
		SA-5: Premature Termination of Critical Data Collection	n/a –The criterion is expected to be satisfied at the time the indications are consulted. Therefore, even though the task description states this as a monitoring activity, the data need only be collected once.
		RP-1: Misinterpret Procedures	n/a – The criterion to be evaluated is presented in flowchart logic and the numerical criteria are explicitly provided. If the data has been correctly assessed, there is a negligible chance of misinterpreting the criterion.
		RP-2: Choose Inappropriate Strategy	n/a – There are no alternatives.
		E-1: Delay Implementation	n/a – Success for this task is a transfer to a path on the CSFST, not an implementation of a response. The CFM is intended for a delay in implementation once the correct response has been identified.
		E-2: Critical Data not Checked/Monitored with Appropriate Frequency	n/a – The data are to be collected once.
		E-3: Fail to Initiate Execution	n/a – This step is a status assessment (decision) step and does not involve execution.
		E-4: Fail to Execute Simple Response Correctly	
		E-5: Fail to Execute Complex Response Correctly	
		AP-1: Misread or Skip Critical Step(s) in Procedure	n/a – The CSF status tree is a single page with a simple logic presented in a flowchart format.

Table 6-5. CFMs identified as applicable for the example HFE

Crew failure path	Tasks or activities	CFMs identified as applicable
Crew failure path #1 failure of Node 4, "Enter FR-H1" (critical task)	Task 1: Monitoring the CSF Status Tree for Heat Sink Criterion 1 "NR Level… Section 4.4.3.1 describes all tasks for Node 4.	**SA-2** Wrong Data Source Attended to **is potentially applicable.** WR levels could potentially be attended to instead of NR levels. They will indicate larger percentage values. **SA-3** Critical Data Incorrectly Processed/Misperceived **is applicable** (for NR Level of SG)**.** The SG level NR value expressed as a percentage may be misperceived.
	Task 2: Monitoring the CSF Status Tree for Heat Sink Criterion 2 "Total AFW Flow…	**N/A:** SA-2 Wrong Data Source Attended**.** There are several indications for assessing whether AFW is operating and all indications would point to zero flow. **N/A:** SA-3 Critical Data Incorrectly Processed/Misperceived (for Total AFW flow criterion). There will be a clear indication of zero flow. N/A: RP-1 Misinterpret Procedures **is n/a**. Once both criteria have been assessed correctly, the flowchart representation of the logic is simple enough such that the red path assessment directly follows. N/A: RP-2 Choose Inappropriate Strategy **is n/a**. The red path assessment provides for no alternatives.
Crew failure path #2 failure of Node 5, "Decision to initiate F&B and transfer to FR-H1 Step 10" (critical task)	Evaluate the criteria listed in FR-H1 Step 2, entitled "Check secondary heat sink" and go to FR-H1 step 10	**SA-3** Critical Data Incorrectly Processed/Misperceived **is potentially applicable.** The critical data (wide range level in SGs) have to be collected and compared against numerical criteria provided in the procedures. A misreading is possible. N/A: **SA-2** Wrong Data Source Attended to **is n/a.** The task involves the SG WR Levels and PZR Pressure indicators. Although SG NR Level may be read instead of WR Level, they will show a lower reading and the criterion will be judged as satisfied. N/A: RP-1 Misinterpret Procedures **is n/a**. This is a simple transfer with no further decision required.
Crew failure path #3 – failure of Node 6, "Implement F&B per FR-H1 Steps 10-13" (critical task)	Steps 10 through 13(of FR-H1). Actuate SI and establish bleed path Section 4.4.3.3 describes all tasks for Node 6.	**E-4** Fail to Execute Simple Response Correctly **is applicable.** The actuation is considered a simple response because it has only two essential tasks, initiate SI and establishing a bleed path via the PORVs. Further there are intermediate steps to verify the effectiveness of the actions. N/A: **E-3** Fail to Initiate Execution **is n/a.** At this stage the crew is focused on the F&B as its immediate priority. **E-1** Delay Implementation is **potentially applicable.** There may be a reluctance to activate F&B because of the long term effects on the plant. However, the transfer step calls attention to the caution before Step 10, which instructs the crew to perform Steps 10-13 quickly.

6.3.3 Application of the DTs to Quantify Crew Failure Paths

Having identified the CFMs applicable to the critical tasks, the next step is to apply the decision trees associated with the CFMs. Recall that in applying the DTs to quantify the probability of a CFM, specific to a task of a critical task, the error correction potential (shown in Table 6-3 for the critical tasks) if applicable is already included in the assessment of the contribution to the HEP

In this example, the SA-2 and SA-3 CFMs are applicable to the first CRD failure path, based on the failure of Node 4. These are both associated with the first task, but were considered not to be applicable to the second task because of the nature of the indications.

For the second CRD failure path, based on the failure of Node 5, the applicable CFM is SA-3. Finally, for the third failure path, based on the failure of Node 6 and dealing with the implementation of F&B, the applicable CFMs are E-1, Delay Implementation and E-4, Fail to Execute Simple Response. An overview of these CFMs is shown in Table 6-6, which summarizes the calculation of the combined HEP.

That there are few CFMs that are relevant to this HFE is a function of the fact that this is a straightforward response that is clear and therefore would be expected to have a low probability of failure. The feed and bleed example presented in Appendix A provides a case where the information available to the crew is misleading, and additional CFMs are brought into play.

Table 6-6. CFMs and error correction potential to be quantified for the example HFE

CRT path	CFM	Error correction
#1 – Failure of critical task / Node 4	SA-2	Node 7
	SA-3	
#2 – Failure of critical task / Node 5	SA-3	Node 8
#2 – Failure of critical task / Node 6	E-1	Node 9
	E-4	

The DTs are applied for each of the CFMs identified for the HFE, as shown in Table 6-6. For each DT application or evaluation, the answers for the DT branch points and their justification are shown in Table 6-7. The justifications shown in this table summarize information from the CRD documentation. As shown in Chapter 5, the DT branch points are determined by answering the questions associated with these. In some of the justifications shown in this table, it can be seen that the DT evaluation may require additional information to be obtained that was not initially in the CRD documentation. With regard to the modeling of error correction, the recovery potential is not credited in most DT evaluations of this example even if the recovery potential has been included on the CRD and a limited basis for the potential is documented for the critical tasks (Nodes 7, 8, 9). The principal reason for this is that there are no truly independent opportunities to correct the errors. To actually credit recovery and especially the recovery in multiple CFMs and tasks, the timeline of the specific failure paths should be reviewed carefully and opportunities for recovery that are sufficiently independent identified as discussed in Section 5.15.

Table 6-7a. Documentation of the DT evaluations. Node 4, task 1, CFM SA-2

CFM	Applied to		Justification
SA-2 Wrong Data Source Attended to	Critical Task 1 of Node 4		The indications for WR SG levels could be attended to instead of NR level indications. They will indicate larger percentage values, leading to delay in the satisfaction of the criterion being evaluated.
	DT Branch Point	Answer	
	1: HSI	GOOD	NR and WR SG Level indications are collocated but labeled clearly
	2: Workload	LOW	This task is performed by the STA, without the need for support from the other crew members, who are attempting to align AFW per ES-01.
	3: Familiarity with the Data Source	GOOD	NR and WR SG Levels
	4: Recovery potential	NO	The recovery potential is based on the CSFST. If the crew determines that they cannot establish FW flow while in ES-01, they would relay this to the STA monitoring the CSFST. Crediting this potential therefore depends on the time at which this information is relayed to the STA. For the purposes of this example, even though a case could be made, recovery is not credited.
SA-2 branch #15 applies. Probability = 1.2E-4 (mean value)			

Table 6-7b. DT evaluation: Node 4, task 1, CFM SA-3

CFM	Applied to		Justification
SA-3 Critical Data Incorrectly Processed/Misperceived	Critical Task 1 of Node 4		The SG level NR value expressed as a percentage may be misperceived.
	DT Branch Point	Answer	
	HSI / Environment	GOOD	The SG levels have been rapidly decreasing since the reactor trip. SG Low-Low levels alarms occurred previously (1 minutes after the loss of feedwater).
	Workload	LOW	Same justification for WORLOAD as for CFM SA-3 for Task 1 of Node 4.
	Training	GOOD	Checking the CSFST is frequently performed and is one of the responsibilities of the STA.
	Recovery potential	NO	For the same reason as discussed for SA-2, Recovery is not credited. (If credited the mean probability for the CFM would be 3.4E-5.)
SA-3 branch #15 applies. Probability = 1.3E-5 (mean value)			

Table 6-7c. DT evaluation: Node 5, CFM SA-3

CFM	Applied to		Justification
SA-3 Critical Data Incorrectly Processed/Misperceived	Critical Task of Node 5		The data have to be collected and compared against numerical criteria provided in the procedures. A misreading is possible.
	DT Branch Point	Answer	
	HSI / Environment	GOOD	The critical data to be read are SG WR Levels; the PZR Pressure is assumed at this point to be within the normal range. It is the SG level that will determine the need to go to F&B. These are primary indications that are frequently used through their full range (when trained emergencies are included).
	Workload	LOW	Workload is consistent with training. While the crew is trying to restore AFW in parallel, only one safety function is challenged and the crew's focus is on ensuring adequate cooling (no extra cognitive distractions).
	Training	GOOD	Checking Secondary Heat Sink is a task that is required in routine as well as emergency situations.
	Recovery potential	NO	The recovery potential is not credited.
SA-3 branch #15 applies. Probability = 1.3E-5 (mean value)			

Table 6-7d. DT evaluation: Node 6 CFM E-1

CFM	Applied to		Justification
E-4 Fail to Execute Simple Response Correctly	Execution		The potential for there to be reluctance to initiate feed and bleed needs to be explored.
	DT Branch Point	Answer	
	Reluctance and Viable Alternative	ABSENT	The crew is trained not to delay once the criteria are reached, and not to wait for a potential recovery of AFW
	Assessment of Margin	Correct	The crew understands that they have some time margin to respond, but the concern for literal compliance with the procedures is the determining factor here.
	Additional Cues	N/A	Not addressed on the tree for this path
E-4 branch 7 applies. Probability = 1E-04			

NOTE: The expert elicitation did not result in a value for this crew failure scenario. The value of 1E-04 is used here for illustrative purposes only.

Table 6-7e. DT evaluation: Node 6, task 1, CFM E-4

CFM	Applied to		Justification
E-4 Fail to Execute Simple Response Correctly	Execution		The task (Actuate SI and open PORVs) is a simple manipulation.
	DT Branch Point	Answer	
	HSI	NOMINAL/ GOOD	The SI and PORV controls are clearly separated and indicated.
	Workload	HIGH	The high workload is being attributed to the relative urgency of establish F&B. The caution note before Step 10 indicates Steps 10-13 should be performed quickly.
	Recovery potential	YES	The procedural steps, Step 11 and Step 13, instruct the crew to verify that SI has been established and to verify the bleed path is adequate and specify the indications to be checked. Thus the feedback is immediate.
E-4 branch 6 applies. Probability = 1.6E-6 (mean value)			

6.3.4 Calculation of the Combined HEP for the HFE

The combined HEP for the HFE is calculated using equation 3 in Chapter 6. The combined HEP is the sum of the CFM probabilities for each CRT path, and the sum of the CRD path probabilities; this is equivalent to a sum of all CFM probabilities. The results for the example are shown in Table 6-8.

In this case, the combined HEP is 2.43E-4. This example does not fully illustrate the value of applying IDHEAS in that it has not exercised many of the decision trees. Its purpose was to provide a simple example demonstrate how the method is applied, and in particular, how the relevant CFMs are identified and the appropriate paths on the DTs are determined on the basis of the PIFs. However, it does illustrate that, for an HFE that is not considered to be challenging, that a low HEP can be supported by a qualitative analysis that shows that there are few relevant CFMs and that their probabilities are low because of the PIFs corresponding to the scenario.

Table 6-8. Quantification of the combined HEP for the HFE

CRT path	CFM	Error correction	CFM branch	CFM Prob.	Path Prob.
#1 – Failure of critical task / Node 4	SA-2	Node 7	#15	1.2E-4	1.3E-4
	SA-3		#11	1.3E-5	
#2 – Failure of critical task / Node 5	SA-3	Node 8	#11	1.3E-5	1.3E-5
#2 – Failure of critical task / Node 6	E-1	Node 9	#7	1E-4	1.0E-4
	E-4		#6	1.6E-6	
HFE probability, point estimate (sum of CRT failure path probabilities)					2.43E-4

The combined HEP for the HFE at this stage represents an initial estimate of the HEP. It reflects conservative assumptions that may be revised if additional information and justification is obtained. More importantly, it does not account for dependencies with other HFEs. In the next steps of the analysis, the HEPs are integrated into the PRA model. The next chapter, “Model Integration”, discusses these. The cut set review and reasonableness check provide importance information, which may be used to determine whether the HFE addresses the expected issue or whether additional information needs to be collected to refine the HEP estimate. The model integration may also identify HFEs appearing in the same PRA failure sequence (cut set), which will require the evaluation of dependencies.

If the contributions from all the CFMs are assessed to be from the lowest branch on the corresponding decision trees, this would reflect the fact that no specific challenging PIFs have been determined. If the HEPs evaluated for each of the contributing CFMs were simply summed then the overall HEP would be a function of the number of CFMs identified. It is questionable whether this is truly an appropriate approach. An alternative could be to replace the sum by a suitable lower bound HEP value that corresponded to a more holistic assessment.

7 MODEL INTEGRATION

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: overall PRA results review and reasonableness check, recovery, dependency, and uncertainty. 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 provided based on the qualitative and quantitative methods developed for IDHEAS. This chapter is an area for future research.

7.1 Results Review and Reasonableness Check

The ASME/ANS PRA Standard requirement HLR-HR-G6 specifically requires the analyst to check the consistency of the HEP quantification by reviewing the final HEPs relative to each other and relative to the given "scenario context, plant history, procedures, operational practices and experience" [1]. A reasonableness check should be done at two levels: 1) consistency within the HFE, and 2) consistency between HFEs (relative risk ranking). The scenario context of an HFE is derived from the accident sequence or accident sequence cut set depending on the level at which the HFE is included in the PRA model. While the PRA Standard describes this reasonableness check being done at the end of the HRA process, a best practice is to conduct reasonableness checks throughout the HEP development process.

Consistent with the PRA Standard, the most significant HEPs are expected to have been evaluated using a detailed HRA approach. Importance measures can be used to identify which HFEs to examine more closely. Those HFEs with the highest Risk Reduction Worth or Fussell-Vesely Importance will have a bigger impact on reduction of the risk metrics such as core damage frequency. In an analogous manner, those HFEs with the highest Risk Achievement Worth will result in a larger increase in the risk metrics.

The first check entails a reasonableness check between the qualitative analysis and the quantitative analysis for a given HFE. This is a "sanity" check that the quantitative result adequately reflects the qualitative insights. If the HEP is lower than reasonably expected given the scenario context implied by the accident sequence or a specific accident sequence cutset, plant history and operational practices and experience, this is an indication that the quantification method was either misapplied or inappropriate assumptions/decisions were made and the quantification should be revisited, *or* that the quantification method is incomplete for that application. In the case of IDHEAS, the latter may occur when the method is applied beyond the internal events, at-power context. If this occurs, changes to the method to introduce new PIF characteristics may be proposed. If the HEP is higher than would be reasonably expected given the scenario context, plant history and operational practices and experience, the analyst may choose to refine the HFE to better or more realistically represent its requirements or revisit the assumptions made in applying the decision trees. Of course, appropriate documentation of the basis for any changes should be provided. Similarly, if the contribution from the decision trees seems unreasonably high given the context (e.g., long time frame, extra crew available for review, simple diagnosis, etc.), the analyst may revisit the recovery credit applied to the HFE.

The second type of reasonableness check – check of consistency between HFEs appearing in different accident sequences or accident sequence cut sets – can be performed after the initial quantification of individual HFEs and before the dependency analysis. However, it should also be revisited once the dependency analysis has been completed. Checking the consistency between HFEs is typically accomplished by sorting the HFEs by HEP and asking: does the relative ranking make sense, given the qualitative analysis and the nature of the tasks. When applying IDHEAS, since the first reasonableness check should have resulted in ensuring that

the quantitative analysis of each individual HFE has been performed consistently with the qualitative analysis, the consistency check should focus to a large extent on the degree of consistency in the assessment of the PIF characteristics from PRA scenario to scenario.

Finally, the review of the results is an important activity in the dependency analysis and is performed to identify those cutsets and those accident sequences to which they contribute that contain multiple HFEs, since they define the context within which dependency needs to be evaluated.

7.1.1 Iteration with Accident Sequence Development

In the majority of cases, the analysis of the HFEs identified during the development of the PRA accident scenarios would not result in restructuring the PRA logic model. However, there may be circumstances where restructuring the accident sequence models or redefining HFEs may be advantageous. One reason for redefining HFEs is to deal with dependence. When two or more responses are directed by the same procedural guidance, they are guided by common cognitive activities. In this case it may be useful to separate the cognitive and execution contributions to the HFEs to simplify the dependency evaluation. A more significant structural change to the PRA model occurs when, during the analysis of an HFE, the existence of negative PIFs identified as significant to determining the HEP can be associated with equipment failures not typically included in the logic model because they do not have a direct effect on accident sequence development. Instead, their effect may be indirect in that they have an effect on operator performance. Such effects can arise when the failures affect the availability or accuracy of indications needed for correct response for example. In such cases, it may be useful to modify the PRA logic model to explicitly incorporate these failure scenarios so that the appropriate probabilistic weight can be associated with the corresponding HEPs. In practice, process of CRD development and CFM evaluation can highlight when HFE definitions may need to be refined or split into multiple HFEs.

For example, in the F&B on LOFW example presented in Section 4.4, the time available for F&B varied based on how the reactor was tripped: a manual trip in 45 seconds yielded a 45 minute time window for F&B, whereas an automatic reactor trip would only allow a 13 minute time window for F&B. Considering the analysis shows that the time required for completion is 25 minutes, this becomes a key distinction, and the HFE may need to be split or refined to explicitly account for the boundary condition of how the reactor was tripped.

7.1.2 Documentation

The process of gathering information, assessing the HFE and integration with the PRA often requires some iteration. To ensure that the HRA is integrated correctly into the PRA and to facilitate the reasonableness check, it is essential that the analysis of each HFE be documented appropriately. Examples of this documentation are provided in Appendix A. This documentation should include:

- The PRA Scenario Description and the expected operator response
- The HFE Definition based on the success criteria for the response
- A task analysis as documented in the Crew Response Diagram (CRD) and the characterization of the nodes in terms of the critical tasks
- A timeline of the critical events (e.g., arrival of cues, time to reach a specific point in the procedure, time taken to execute a response, etc.)
- Detailed task analysis of CRD nodes identifying the activities that are used to identify CFMs (see tables in Chapter 4 for the task analysis)
- Evaluation of Crew Failure Modes (CFMs) using the associated Decision Trees (DTs),l and a justification of the choice of path through each DT

- Estimation of HEP
- Summary of analysis and key insights

7.2 Recovery Analysis

Recovery actions are included in the PRA "…on an as-need basis to provide a more realistic evaluation of significant accident sequences…" [1]. Operator actions can be credited to restore functions, systems or components; to do this, operator recovery actions should restore failed equipment or find alternative equipment or configurations within the time period required [2]. Significant recovery actions may be evaluated through the same process as all other HFEs (i.e., feasibility, qualitative analysis using CRTs, quantitative analysis using the DTs, and then model integration, including uncertainty and dependency) when it is considered important to do so to provide additional justification for the credit assumed.

These actions to restore functions, systems or components are new basic events that would be added to the PRA, not to be confused with the "recovery" of an HFE which is credited within the decision trees. Recovery mechanisms such as peer checking, unexpected instrument responses in response to an action, and new alarms that correct an error in response and would prevent the HFE from occurring are typically credited in the evaluation of the HEP for the HFE, and not modeled explicitly as separate basic events in the PRA model.

Repair of components, meaning the restoration of a failed SSC by correcting the failure and returning the component to operability is typically quantified using empirical data (if credited at all) and is not treated using HRA techniques.

7.3 Dependency Analysis

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.

7.3.1 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.

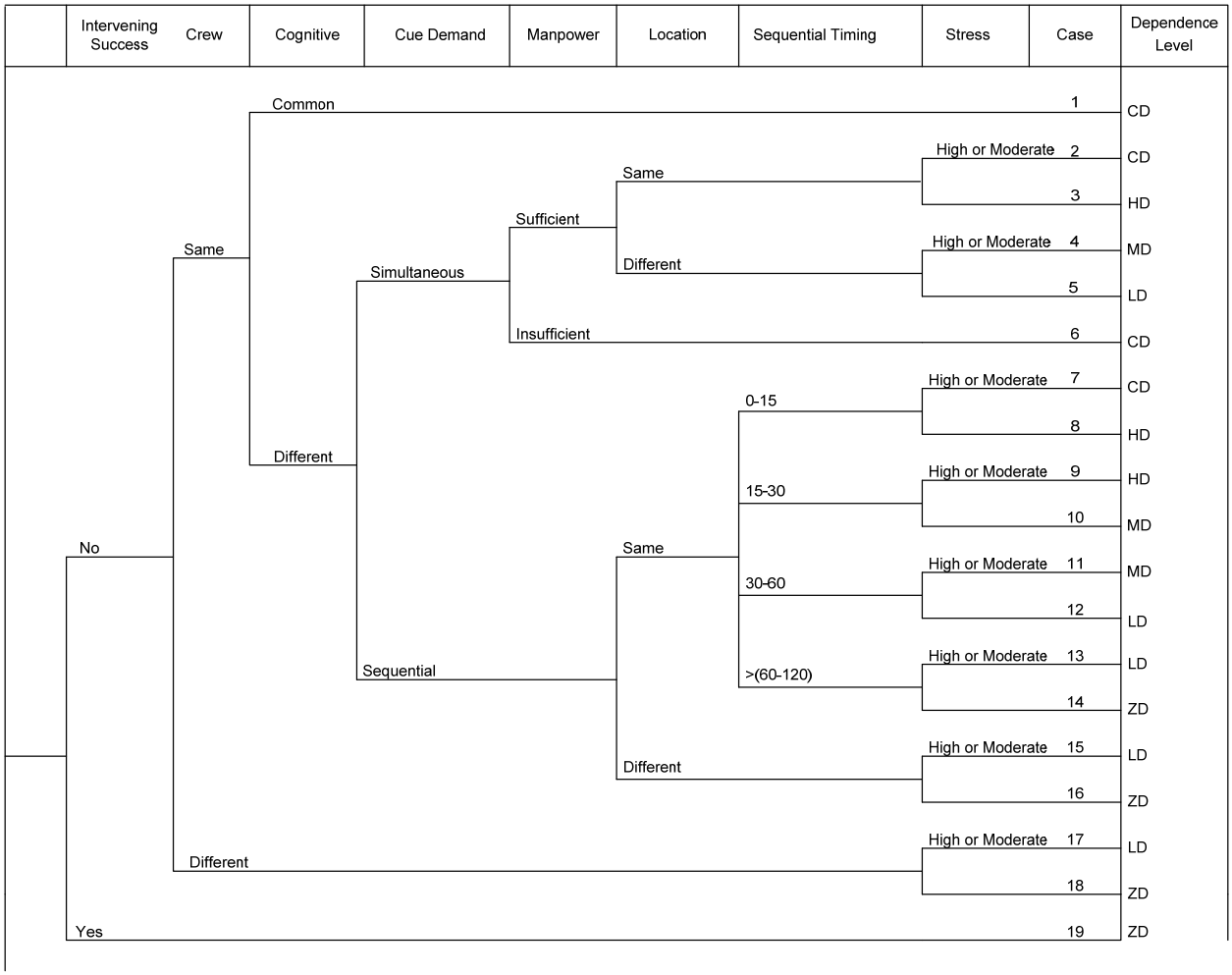


Figure 7-1. Diagram of dependency levels. CD – completely dependent, HD – highly dependent, MD – moderately dependent, LD – low dependent, ZD – Not dependent.

7.3.1.1 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*.

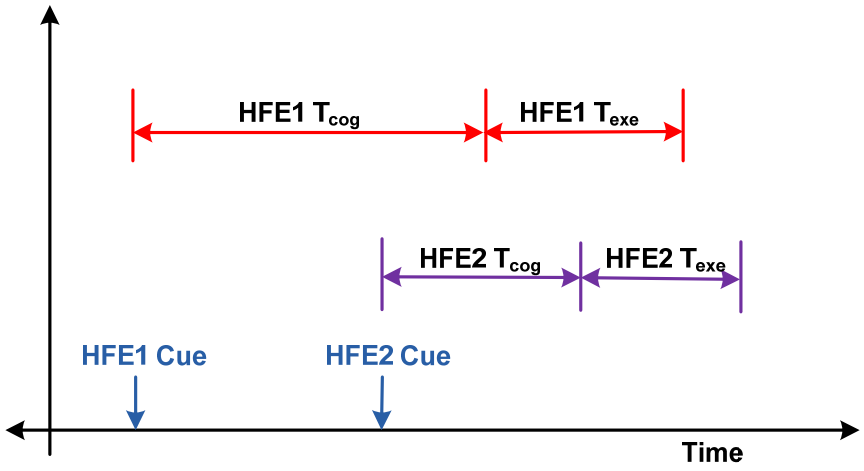


Figure 7-2. Illustration of common cue demands for two HFEs.

- **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

7.4 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.

1. 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 adopt this practice in estimating the probability distribution of the HEPs in its quantification model. The estimation of the HEPs for every DT path was obtained through a formal expert panel; the panel employed the SSHAC process that is to obtain the center, body, and range of the parameters. Therefore, every DT path is associated with a central value of HEP and its distribution. The parameter uncertainty in the combined HEP for an HFE can be represented by combined distributions of the selected DT paths for all the CFMs of the HFE.
2. 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.

During the development of IDHEAS many assumptions have been made. For example, the assumption has been made that the set of CFMs is adequate to represent the potential crew failure modes in internal at-power events. These fundamental aspects of the model cannot be examined without changing the model, which can be cumbersome. 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."

3. 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 SSC 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]

7.5 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.

8 EPILOGUE

The methodological framework developed in the IDHEAS project consists of a detailed qualitative analysis that includes a cognitive task analysis to identify the significant activities (cognitive and execution related) required for success in a response, whose failure is represented as an HFE. This analysis is represented in a crew response diagram (CRD) whose nodes correspond to the critical high level steps or tasks, such as transition between procedures or key steps in a procedure and execution of the response actions. The nodes of the tree are analyzed by identifying the crew failure modes (CFMs) that could result in failure. The set of CFMs and associated Decision Trees (DTs) are the result of condensing the information obtained from the literature survey into a form that is relevant to the analysis of operating crew failures. This can be interpreted as a model of human performance that, for each CFM, identifies the types of PIFs and the characteristics of those PIFs that are considered most influential on the ability of the crew to succeed or fail, based on an underlying identification of the most important cognitive mechanisms.

Areas for future research identified during the development of this guidance fall into roughly two categories:

1. Outstanding technical issues to making this method a practical tool for HRA analysts.
2. Development of an improved approach to dependency analysis using the characteristics of the IDHEAS method.

8.1 Outstanding Issues

The main step that needs to be taken is the further operationalization of the model so that, with the appropriate guidance, it can become a practical tool for HRA analysts. There are several issues that need to be clarified:

1. Ease of use: Applying this model to every HFE in a PRA would be very labor intensive for relatively little gain in understanding. Therefore, if the method is to be widely accepted, there needs to be some sort of screening approach so that the full method is applied only to the significant HFEs, i.e., those that contribute significantly to the results by some defined criterion (in the ASME/ANS standard this is related to its FV and its RAW importance measures). The method in its present form is intended as a detailed HRA approach, and when applied to events identified as risk-significant as determined by the criteria in the ASME/ANS PRA Standard, would be sufficient to meet Capability Category ll. If applied to all HFEs, its application would meet Capability Category III.
2. Level of decomposition: This issue is related more to the development of the CRD and the identification of the critical tasks/activities and the identification of relevant CFMs than it is to the DTs themselves, although it does have a bearing on the way the trees are to be interpreted and used. For many HFEs, there is a natural level of decomposition, in that it is relatively easy to identify the appropriate breakdown. This applies to those cognitive tasks that appear in a linear way, e.g., making a decision based on parameter values follows the successful collection of the relevant data. However, there are some CFMs, in particular: miscommunication; miss a step in the procedure; wrong data attended to, data misperceived, and misinterpret a procedure, which could occur anywhere within the sequence of cognitive task and could occur multiple times. Further, some of the CFMs are only applicable under very particular circumstances. For example, the CFM, dismiss critical data, is only applied when a plant signature can be identified that closely matches the true plant signature. Such scenarios are very rare and would not be encountered for HFEs typically found in PRAs. Additional guidance may be needed on the performance of the cognitive task analysis (developing the CRD and representing the nodes appropriately),

including how to identify critical data, and when and how the CFMs are to be applied. This guidance needs to address and accommodate the different styles of procedures, including the somewhat linear style with transfers to event specific procedures adopted by Westinghouse and the flowchart style adopted for BWRs.

3. Quantification: The proposed quantification approach builds up the HEP from the probabilities of the contributing CFMs. For many HFEs it can be expected that the nominal, i.e., most optimistic path through the DT has been taken. If this is the case, there is no real explanation of why the failure or its constituent CFMs occurred from a contextual point of view; i.e., the context is not error forcing in any sense. Taken at face value, the HEP would be proportional to the number of CFMs that were used in the evaluation of the nodes of the CRD. One issue that needs to be resolved is whether there needs to be a renormalization of the lowest HEPs to result in reasonable lower bounds on the total HEP since it might be unrealistically high. An approach which would be similar to that taken in the MERMOS method for example would be to use the HEPs generated by the method directly when there is an error forcing context (at least one of the PIFs is negative) but include a lower bound HEP when an error forcing context cannot be identified.

8.2 Development of an improved approach to dependency analysis using the characteristics of the IDHEAS method

8.2.1 Dependencies between HFEs

To model dependencies between two HFEs, we need to first understand how the first HFE may affect the failure of the second. From a cognitive perspective, the root causes of human errors include (but are not necessarily limited to) the following:

1. Task demand exceeds the cognitive resource limits, or approaches the boundary conditions of underlying cognitive processes. Such limits and boundary conditions were identified as cognitive mechanisms underlying human errors in IDHEAS development.
2. PIFs modulate task demands, cognitive limits, and boundary conditions.
3. The crew fails to detect and recover the errors.

IDHEAS models an HFE by identifying the critical cognitive tasks and response activities in the HFE and addresses potential task failures through the use of CFMs. The CFMs address the way the crews could make errors during situation assessment, response planning, and response execution that could lead to the failure of the HFE. Each CFM uses a DT to model the effects of plant and scenario conditions and various PIFs (which taken together are the PIFs described in the DTs) that could contribute to the potential for the CFM occurring, along with the potential for recovering the CFM if it did occur. For a given HFE, analysts first identify the critical tasks/activities and the potential CFMs for the tasks, then identify the path through the DT for each of the CFMs. The paths address the potential contributors to failure, with the end point of the path reflecting the probability of the CFM given the conditions present (context). With a traceable causal structure like this, the effects of a prior event on the error causes in subsequent events can be identified by systematically examining the nature of the CFM(s) determined to be most likely to have an impact in the first HFE (e.g., CFMs related to situation assessment or response planning or response execution) and the existing plant conditions and PIFs contributing to the key CFMs that could be relevant to subsequent HFEs. Thus, the IDHEAS approach offers a way to better understand the potential reasons for a failed HFE and thereby provides a better understanding of the context for subsequent events. It also allows for separate consideration of diagnostic and execution failures both on the initial HFE and the subsequent HFE, rather than assuming a particular failure would affect both.

More generally, the IDHEAS approach helps:

- develop a complete picture of the scenario to see where and when the operators are required to respond, when the cues come in (because the context for the HFEs will change as the sequence develops, and what is true at the time of the first response may not be true at the time of the second).
- understand why and how the first HFE might have failed, how the failures may change the context as the scenario evolves, and how the changes will affect the task demands, cognitive resources, and PIFs of the tasks or CFMs in subsequent events.
- understand the cognitive processes underlying the CFMs and use the cognitive mechanisms to examine the dependency effects.

With such information, the dependency context between two events can be better understood. However, what still needs to be developed is a set of rules to determine dependency levels between events given the information obtained through the IDHEAS approach and guidance for determining the quantitative effect of the conditions (context) on the HEP of the subsequent events.

8.2.2 Dependencies within HFEs

It should be noted that IDHEAS has already implicitly addressed dependencies within an HFE. As discussed above, IDHEAS analyzes an HFE as a set of critical tasks, each task being characterized with a set of CFMs, and each CFM being applicable to a set of task characteristics and influenced by specific PIFs. The dependencies between the elements of each set have been treated as follows:

- CFMs were developed as being non-overlapping;
- The dependency across critical tasks is addressed through consideration of workload, which considers the effects of multitasking, interruption, disruption, timing, and cognitive fatigue from other tasks on the task being analyzed;
- The potential for recovery (i.e., a correction made before the failure of the function occurs) is dependent on the way the crew fails, i.e., the CFM.
- Dependencies between the PIFs are treated by the fact that the effect of a PIF combination on the HEP of the CFM is addressed through direct or interpolated judgments obtained during the expert elicitation performed to obtain the HEPs.

Appendix A. Example Application of IDHEAS Method

As part of the development process, three example HFEs were evaluated using the IDHEAS methodology. These analyses are documented here in a manner that provides a complete narrative of the evaluation that included the following: documentation of the analysis of the HFE in the form of a CRD including definition of the CRD nodes; associated timeline; determination of the applicable CFMs for each node of the CRD and evaluation of the corresponding DTs; and finally the quantification of the total HEP and examination of the risk insights. Note that the analysis is performed in an iterative manner; in particular the identification of the expected procedural path, the construction of the CRD and the associated timeline are performed at the same time and provide an integrated assessment of the HFE. The linear presentation of the analysis results should not be taken to mean that this is a simple linear process; however, each of the components needs to be documented clearly.

The three examples documented here are for illustrative purposes and the HFE definitions may have been modified from their original source in order to simplify the analysis or illustrate a particular point of the method. All examples are from (different) PWR plants using Westinghouse procedures. These examples include:

1. Total Loss of Feed Water with Misleading Indicator (adapted from HFE 1A/B from the US Experimental Study)[18]
2. Loss of RCP Sealwater (adapted from HFE 2A from the US Experimental Study)
3. Fail to Cooldown and Depressurize due to Small LOCA (plant HRA; reference plant, and thus procedures, are different than those used in examples 1 & 2)

Please note, these examples were developed prior to the finalized results of the expert elicitation, therefore, the probabilities provided here are representative values based on the raw data of the expert elicitation. These numbers are in red text and may be in conflict with values reported in the body of the text. In both cases, the main body of the report reflects the most up-to-date information.

Also included in this Appendix is an assessment that was performed for an SDP evaluation, namely the loss of RCP seal cooling following a fire event. This is presented in different format than the first three examples.

A.1 Scenario 1: Total Loss of Feed Water (LOFW) with Misleading Indicator

This scenario is adapted from the NRC/Halden US Experimental study HFE 1 A&B.

A.1.1 PRA Scenario Description, Expected Operator Response and HFE Definition

PRA Scenario: The plant is a four loop Westinghouse plant operating at 100% power. The Shift Technical Advisor is not in the control room. He or she will arrive 5 minutes after being called. The other participating crew members are in the control room (SM, US, 2 ROs). There are three main feedwater pumps: 11, 12 and 13, and four auxiliary feedwater pumps: 11, 12, 13 and 14. AFW pump 14 is turbine-driven and the other three are motor-driven.

[18] Forester, J., Liao, H., Dang, V. N., Bye, A., Presley, M., Marble, J., Broberg, H., Hildebrandt, M., Lois, E., Hallbert, B., and Morgan, T. (2016). Assessment of HRA Method Predictions Against Operating Crew Performance on a US Nuclear Power Plant Simulator (NUREG-2156, Draft Report). Washington, DC: US Nuclear Regulatory Commission.

The scenario begins with the loss of main feedwater; main feedwater pump 11 fails first with the subsequent trip of feedwater pump 12 and 13 within the next 10 seconds. With all main feedwater pumps tripped, if the crew doesn't trip manually the reactor will trip on low SG level (20%).

At autostart, Auxiliary feedwater (AFW) pump 14 overspeeds and causes damage that cannot be repaired. AFW pump 11 has a seized shaft and trip and is not available. AFW pump 13 starts but the shaft shears and no flow will be indicated.

AFW pump 12 starts automatically and indicates full flow, but this flow does not reach (feed) the steam generator because a recirculation valve is mis-positioned (it is open). There is no indication of the valve's position in the control room.

Therefore, there is no AFW flow to the SGs, and the SG levels go down. In reality, criteria to start FR-H.1 are met. However, because of the indicated flow from AFW pump 12, the plant computer will not show a red path on the heat sink status tree.

Expected operator response: The crew is expected by training to trip the reactor in anticipation of an automatic trip on low SG level. If they do not do so, an automatic trip will occur. The expected response is that the crew will transfer from E-0 to procedure FR-H.1, and try to reestablish the heat sink by restoring the AFW function, and if that is not possible, to establish feed and bleed when the WR level on any two SGs are less than 50% with feed from the safety injection pumps and bleed through the PZR PORVs.

In this PRA scenario it is assumed that the operators cannot establish AFW flow even were they to recognize the need to do so, which is complicated by the fact that there is indication of full flow from one AFW pump. Attempting to establish AFW flow to the SGs will be a distraction. There are possible success paths for reestablishing AFW flow:

- Dispatch a plant operator (PO) to check and close the open recirculation valve (feed SG B). However, for this scenario, it is assumed that the valve is stuck and cannot be closed.
- Cross-connect AFW flow from pump 12 to SG A, C or D. The cross-connection can be done from the main control room. However, even if the crew were to try cross-connecting before B&F, the breaker for the power to the valve would open (as part of the scenario) and the valve would remain closed.

Thus the only success path is to establish feed and bleed.

HFE Definition: Functionally the HFE is defined as failure to initiate Feed and bleed before core damage.

According to FR-H.1, B&F shall be initiated when wide range (WR) level on any two SGs is less than 50%.

A.1.2 Crew Response Diagram (CRD) and Task Analysis

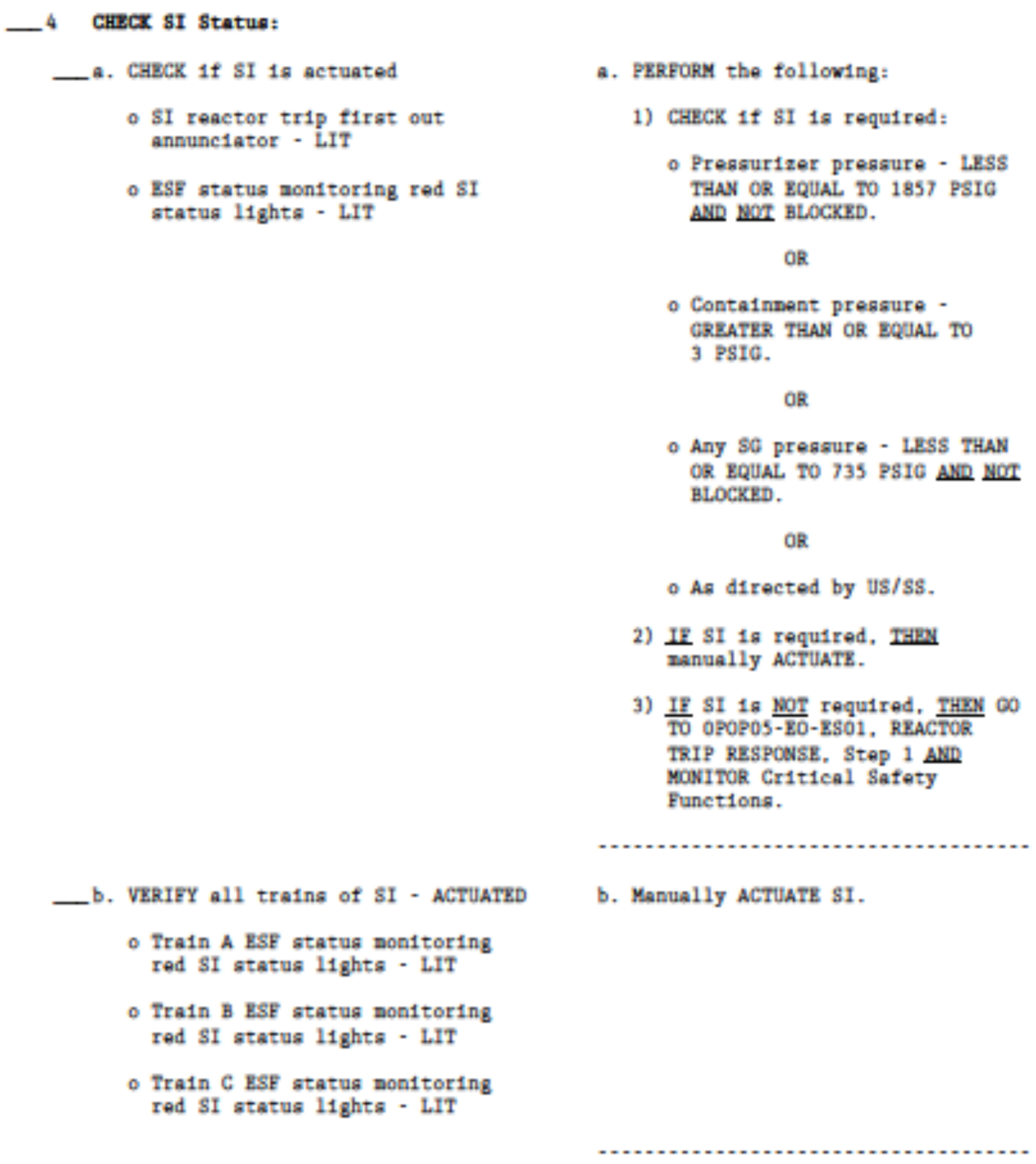
This section outlines the procedural path for success. At T=0 the reactor will trip (manually or auto trip) due to loss of MFW [at least 1 SG showing <20% NR on 2 of 4 channels]. At that point the crew will enter Emergency Operating Procedure E-0 for REACTOR TRIP OR SAFETY INJECTION and will perform the immediate memorized actions (i.e., first 4 steps of E-0). At step 4 of E-0 (Figure A-1) the crew will assess the need for safety injection (SI), and, since no SI had been actuated or is required, they will be procedurally directed to transfer to REACTOR TRIP RESPONSE procedure ES-01 and begin monitoring the Critical Safety Function Trees (CSFTs).

The main cue for the crew to understand they are in a loss of heat sink scenario is the trend of lowering SG levels. Within the first few minutes of entering ES-01 the crew will reach step 3

which directs them to check AFW flow. In this case, flow is indicated. While it is standard practice to confirm flow with level, at this time the SG level is still dropping rapidly, so the operators will not be suspicious of the misleading indication here and will proceed through ES-01.

The crew will continue to progress through ES-01 until they reach step 8 (~T=8). At this point in the scenario, the SG NR level has dropped below 14%, and the STA is in the control room and monitoring the CSFTs, which will be showing a yellow path (figure A-2 below):

Figure A.1.1 Extract of Step 4 of E-0



___4 **CHECK SI Status:**

___a. CHECK if SI is actuated

- o SI reactor trip first out annunciator - LIT
- o ESF status monitoring red SI status lights - LIT

a. PERFORM the following:

1) CHECK if SI is required:

- o Pressurizer pressure - LESS THAN OR EQUAL TO 1857 PSIG AND NOT BLOCKED.

OR

- o Containment pressure - GREATER THAN OR EQUAL TO 3 PSIG.

OR

- o Any SG pressure - LESS THAN OR EQUAL TO 735 PSIG AND NOT BLOCKED.

OR

- o As directed by US/SS.

2) IF SI is required, THEN manually ACTUATE.

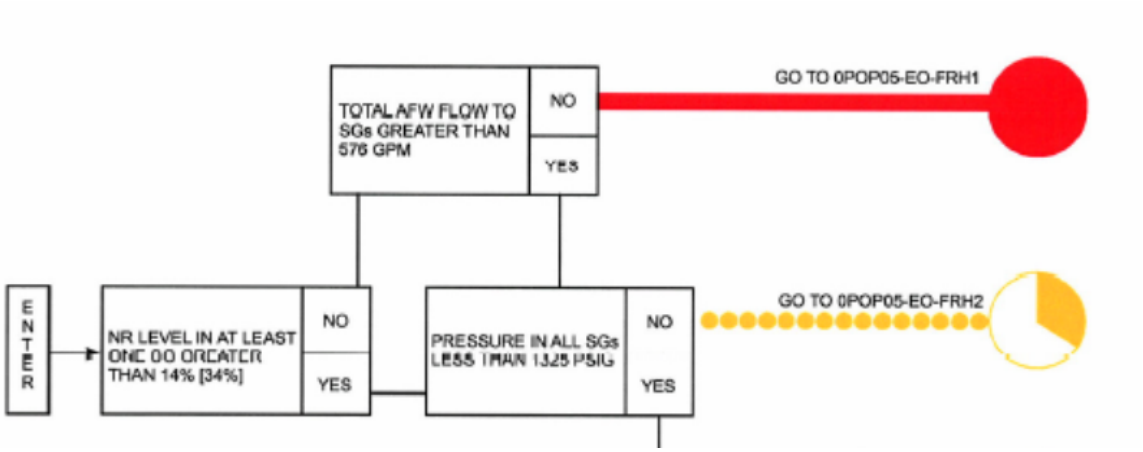
3) IF SI is NOT required, THEN GO TO 0POP05-EO-ES01, REACTOR TRIP RESPONSE, Step 1 AND MONITOR Critical Safety Functions.

___b. VERIFY all trains of SI - ACTUATED

- o Train A ESF status monitoring red SI status lights - LIT
- o Train B ESF status monitoring red SI status lights - LIT
- o Train C ESF status monitoring red SI status lights - LIT

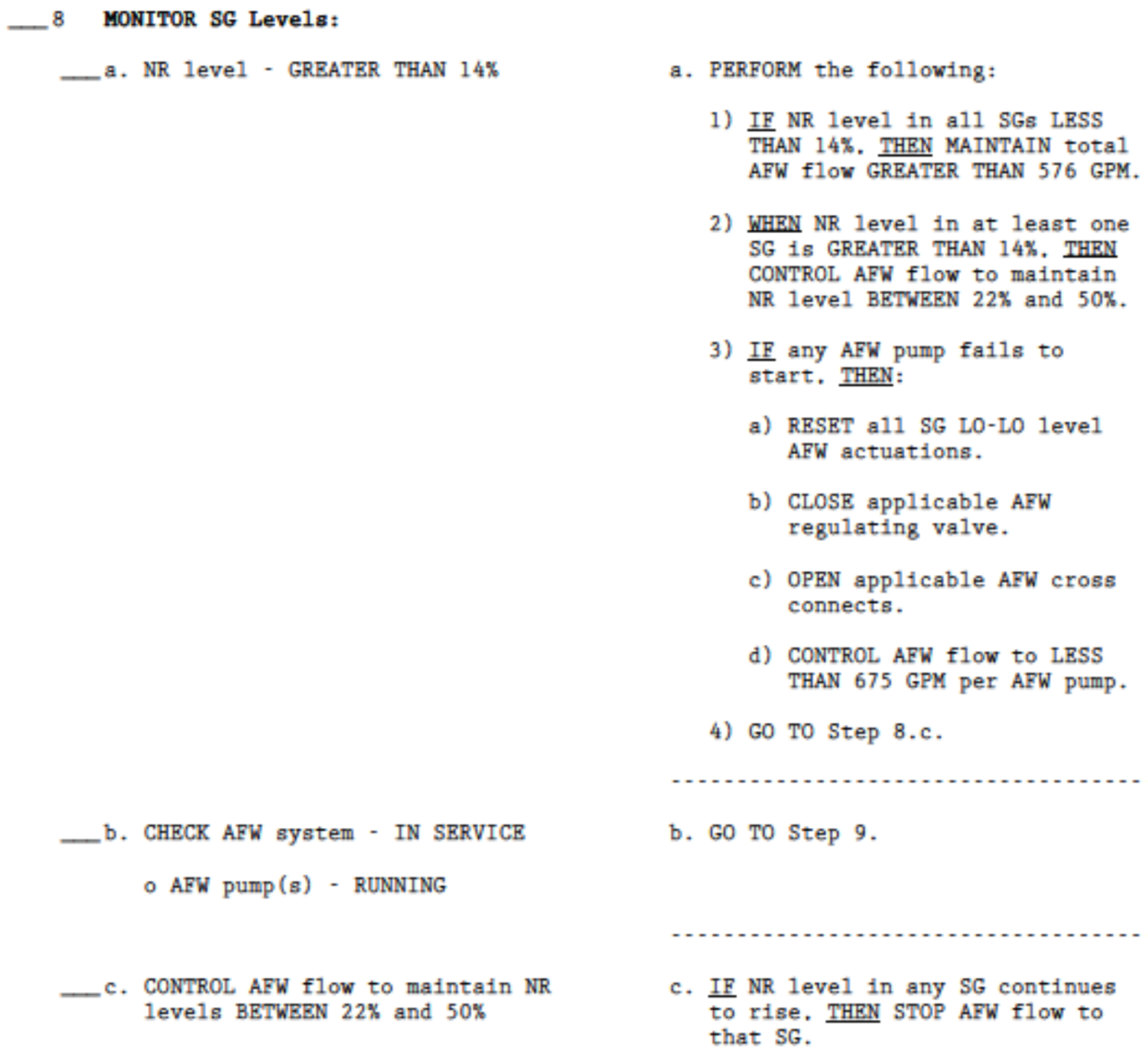
b. Manually ACTUATE SI.

Figure A.1.2. Heat Sink CSFT



Step 8 of ES-01 (figure A-3 below) directs the crew to check if the SG NR Level is GREATER THAN 14%, which, in this case, it will not be. The RNO column will direct them to MAINTAIN total AFW flow GREATER THAN 576 GPM. In this case, because of the misleading indicator, they may think they have adequate flow. As they progress through the RNO column, step 2 directs the crew to control AFW flow to the SG to keep it between 22% and 50%. However, at this point the crew should realize that the NR levels are not increasing, and are in fact decreasing. This will cue the crew that they have inadequate AFW flow and that they are indeed on a red path in the CSFTs. If the crew gets to step 8 before the SG NR levels reach 14%, then they will say yes to step 8a, and will be faced with the same dilemma of attempting to maintain SG levels in step 8c, which they will be unable to do. This step is expected to take several minutes, as the SG levels are dropping slowly.

Figure A.1.3. Step 8 in ES-01

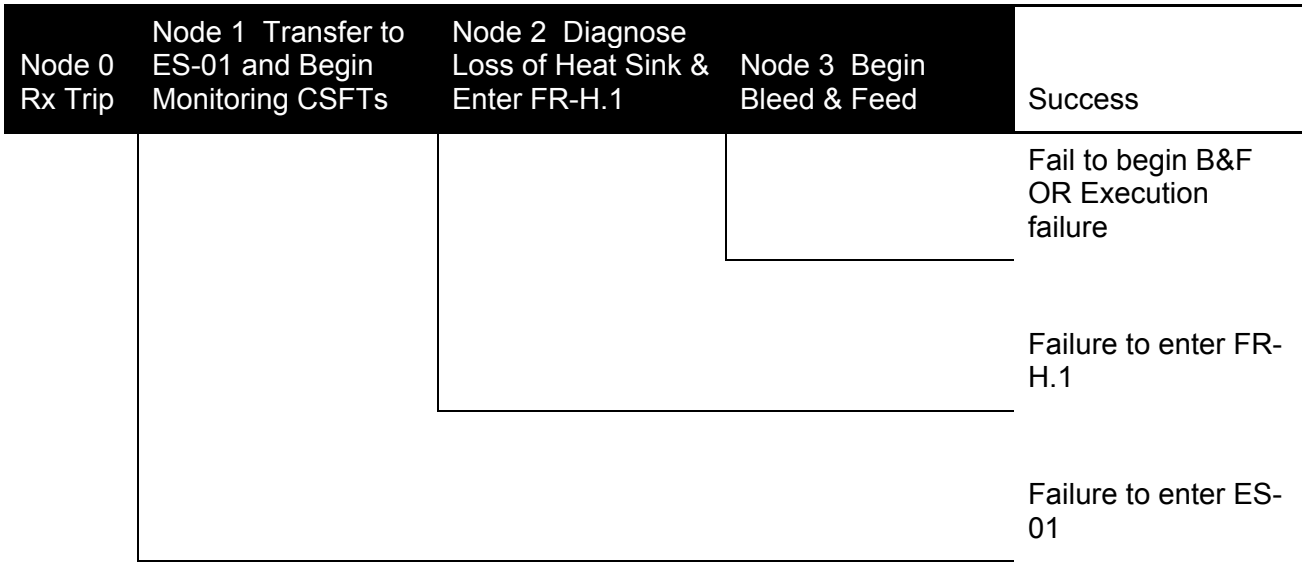


___8 **MONITOR SG Levels:**	
___a. NR level - GREATER THAN 14%	a. PERFORM the following: 1) IF NR level in all SGs LESS THAN 14%, THEN MAINTAIN total AFW flow GREATER THAN 576 GPM. 2) WHEN NR level in at least one SG is GREATER THAN 14%, THEN CONTROL AFW flow to maintain NR level BETWEEN 22% and 50%. 3) IF any AFW pump fails to start, THEN: a) RESET all SG LO-LO level AFW actuations. b) CLOSE applicable AFW regulating valve. c) OPEN applicable AFW cross connects. d) CONTROL AFW flow to LESS THAN 675 GPM per AFW pump. 4) GO TO Step 8.c.
___b. CHECK AFW system - IN SERVICE o AFW pump(s) - RUNNING	b. GO TO Step 9.
___c. CONTROL AFW flow to maintain NR levels BETWEEN 22% and 50%	c. IF NR level in any SG continues to rise, THEN STOP AFW flow to that SG.

Once the crew realizes they have a red path in the heat sink CSFT, they are directed to the RESPONSE TO LOSS OF SECONDARY HEAT SINK functional restoration procedure FR-H.1. The criteria for B&F are SG wide range level in at least two SGs LESS THAN 50% OR Pressurizer pressure GREATER THAN 2335 PSIG. In this case it is likely that the B&F criteria are met at the time of entry into FR-H.1, even for crews that trip early. If the criteria are met, the crew can begin B&F (steps 10-14 of FR-H.1) directly from the Conditional Information Page (CIP). If not, step 2 and then again step 9 of FR-H.1 direct the crew to evaluate the SG WR levels and direct them to step 10 to initiate B&F.

Figure A.1.4 provides a graphical depiction of the crew response diagram (CRD) for this HFE.

Figure A.1.4. Crew Response Tree



The nodes are defined in the following:

Node 0*:* Rx Trip (Auto or manual)

Not Evaluated. Because the timing is so different for the two scenarios (i.e., 13 minute v. 45 minute time window for success) these two cases will be evaluated as separate HFEs in order to illustrate how time constraints can impact the analysis and choice of CFM branch points.

Node 1*:* Transfer to ES-01 and start monitoring CSFTs.

- This is done via Step 4 in E-0

Node 2: Diagnose loss of heat sink and enter FR-H1

- Because of the misleading indication of flow, there is no direct cue, but by continuing to monitor the SG levels in Step 8 of ES-01 and recognizing that they cannot be maintained, the red path on the heat sink CSFT will be attained and they will trandfer to FR-H1.

Node 3: Begin Feed and Bleed

- Steps 10-14 direct the crew to begin feed and bleed

Table A.1.1 Task Analysis Table

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information
1	1	Check indications of RCS integrity and correctly transfer to Es-01, and start monitoring CSFTs	Locate the appropriate indicator(s). Read the numerical value correctly. Understand that the indications are all in the normal range.	See Figure A-1 for specific details
2	2	Attempt to maintain SG levels between 22% and 50%, and failing to do so diagnose loss of heat sink	Monitor SG levels. Read the numerical value correctly. Understand that the indication is above the specified pressure.	Success hinges on recognizing that the SG levels cannot be maintained even though flow is indicated
3	3	Initiate Feed and Bleed	Correctly interpret the procedure Correctly read the WR levels Initiate F&B (a simple task)	

A.1.3 Timeline

Figure A-5 provides a representative graph of SG level vs. time. Initially there is a large drop in the SG level and then the level decreases slowly and steadily. The extent of the initial drop is dependent on the time from the initiating event to reactor trip. Figure A-5a represents an early trip (~30 sec); an automatic trip could see an initial level drop down below 45% WR (figure A-5b). In order to diagnose the lowering SG levels, the crew needs to wait until after the initial drop and after the time at which AFW is expected to kick in before they can notice that the level is actually dropping instead of rising. In general, the earliest the crew can begin to detect the trend is ~T=6min, and it would take some time (~1-2 minutes) to observe the trend due to the slow decrease (~0.5 %/min). For the crew that trips later, the trend becomes discernible sooner in the scenario, so, even though they have a shorter time window, they also have a shorter T_{delay}.

Figure A.1.5. SG level (WR) v. Time [Note: time, in this graph starts at the beginning of the simulator scenario, not at reactor trip (i.e., T=0 is not Rx trip on this graph). Total loss of heat sink occurs at roughly 2 minutes into the scenario and that is the cue for Rx trip].

Figure A.1.5a, early Rx trip (~30 sec after total loss of heat sink):

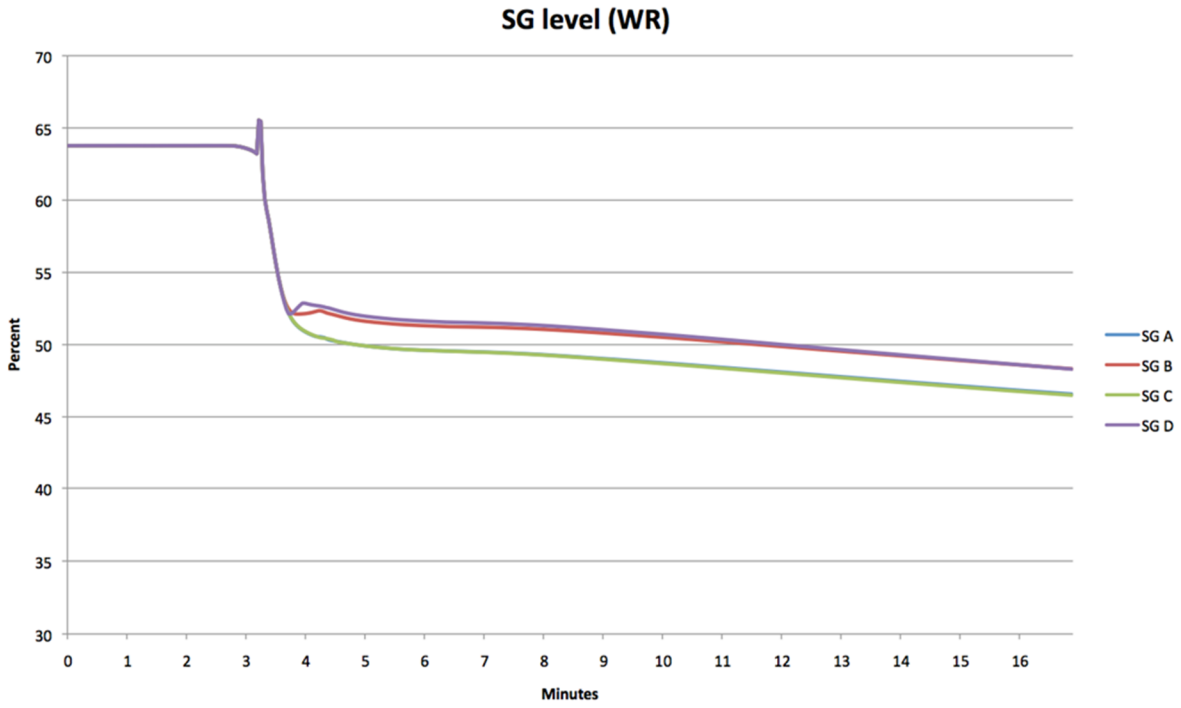
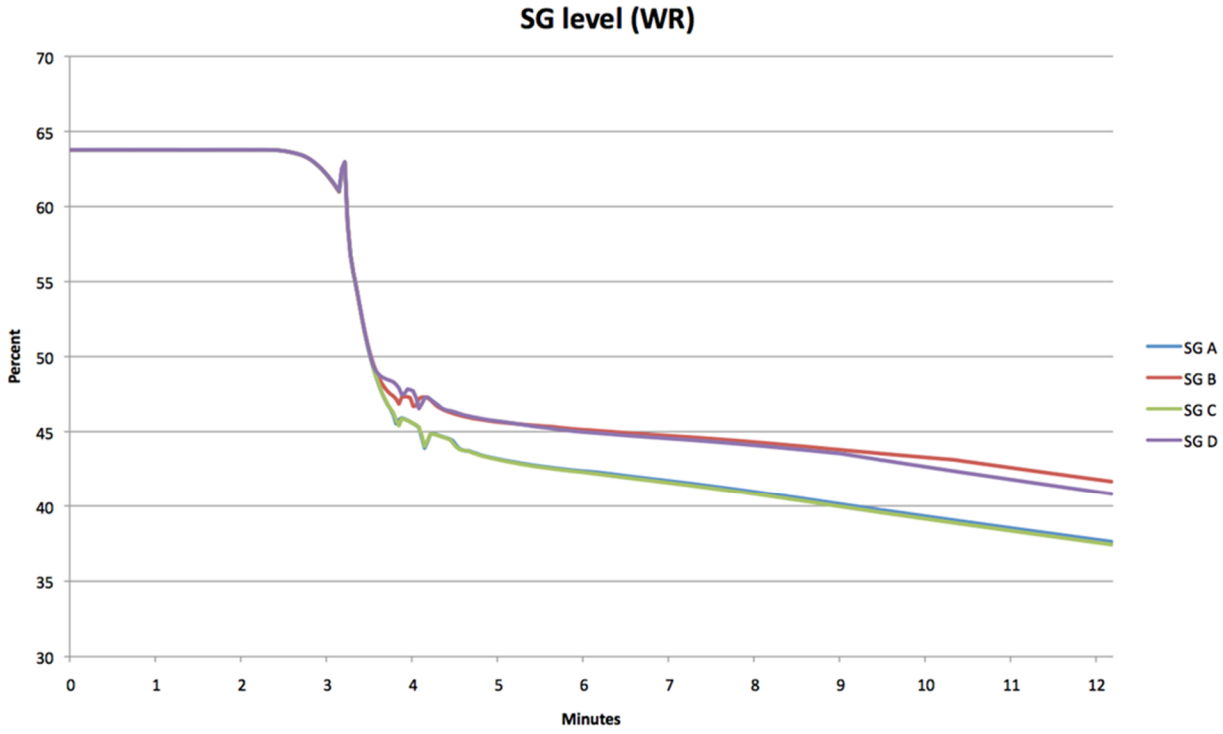


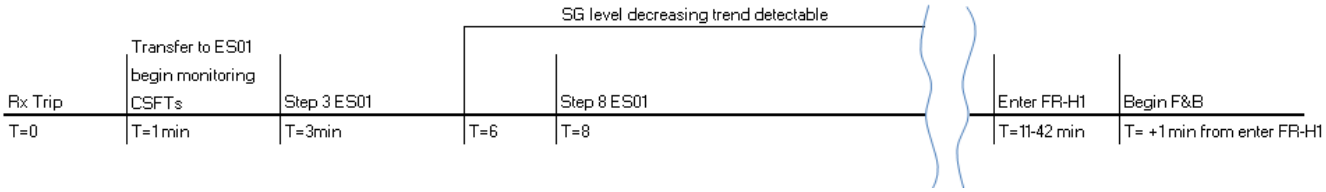
Figure A.1.5b, late Rx trip (~50 sec after total loss of heat sink):



Another consequence of tripping the plant manually versus allowing an automatic trip is the impact on the time available to initiate Bleed & Feed (B&F) before core damage (CD). If the crew manually trips the reactor within approximately 30 - 45 seconds of the loss of feed water,

they will have approximately 45 minutes before CD. If they fail to manually trip, the plant will trip automatically on low-low steam generator (SG) narrow range (NR) level (20%) approximately 50-60 seconds after the loss of feed water. If the plant automatically trips on low-low SG level, the crew will have about 13 minutes to initiate B&F to avoid CD.

Figure A.1.6. Timeline



Based on discussion with operations personnel the above timeline has been established and the response is considered to be feasible: the time required is 12 minutes (average) and the time available is 13-45 minutes. While both the long (45 min) and short (13 min) time frame scenarios are feasible, the same recovery opportunities are not applicable to both scenarios. Note: the trend of the SG level decreasing in combination with Step 8 is reached in time for the crew to act in the short time frame scenario, however, the time available to spend in Step 8 trying to understand why they cannot control the SG level is substantially shorter (~4 minutes vs. 36 minutes). The impact of this difference will be evaluated during the CFM evaluation.

A.1.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees (DTs)

Table A.1.2 CFM selection table – Critical task 1

CRD Node	1 – Transfer to ES-01	
Critical Task	1 – Check indications to determine whether SI is required. Note: Since there are several indications that need to be checked, SA-2 and SA-3 apply to the activity associated with each of these indication checks.	
CFMs	Applicable? (Yes/No)	Justification
AP-1: Key Alarm not Attended to	No	n/a. Response of this node is to a procedural step, not alarm.
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable in principle (Step 4 of E-0). However, this is one of the immediate actions on a reactor trip, and as such it can be screened out.
SA-1: Data Misleading or Not Available	No	n/a. For this PRA scenario there is no misleading data.
SA-2: Wrong Data Source Attended To	Yes	Multiple data sources (see note above)
SA-3: Critical Data Misperceived	Yes	Multiple data sources (see note above).
SA-4: Critical Data Dismissed/Discounted	No	n/a. No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	n/a. Not a monitoring task.
RP-1: Misinterpret Procedures	No	n/a. No viable alternative.
RP-2: Choose Inappropriate Strategy	No	n/a. No viable alternative.
E-1: Delay Implementation	No	n/a. Not an execution step.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	n/a. Not a monitoring task.
E-3: Fail to Initiate Execution	No	n/a. Not an execution step.
E-4: Fail to Correctly Execute Response (Simple Task)	No	n/a. Not an execution step.
E-5: Fail to Correctly Execute Response (Complex Task)	No	n/a. Not an execution step.

Table A.1.3 Assessment of applicable CFMs for Node 1

SA-2: Wrong Data Source Attended to		
PSF	Assessment	Justification
HSI	GOOD	Parameter is an important one, therefore HSI is presumed not to be poor
Workload	HIGH	This is a scenario with multiple failures leading to an initial high cognitive demand. NOTE: However, since this occurs immediately after reactor trip and determining whether SI is needed is a priority, the crew is unlikely to be distracted from this activity. Therefore the assignment of High is possibly conservative, and this is flagged as a source if uncertainty.
Familiarity with Data Source	GOOD	
Recovery Potential	NO	If they don't get into ES-01 there is insufficient time margin to rely on transfer from later steps in E-0
Crew Failure Scenario #		11

SA-3: Critical Data Misperceived		
PIF	Assessment	Justification
HSI/Environment	GOOD	Parameter is an important one, therefore HSI is presumed not to be poor.
Workload	HIGH	This is a very complex scenario with multiple failures leading to a high cognitive demand. NOTE: However, since this occurs immediately after reactor trip and determining whether SI is needed is a priority, the crew is unlikely to be distracted from this activity. Therefore the assignment of High is possibly conservative, and this is flagged as a source if uncertainty.
Training	GOOD	Training on E-0 is good
Recovery Potential	NO	There is no time margin sufficient to allow for procedural recovery
Crew Failure Scenario #		11

Note: This step in the procedure is a memorized step in the procedure and the expected scenario would be one for which there is no need for SI. The CFMs SA-2 and SA-3 need to be assessed for each of the critical parameters: pressurizer pressure; containment pressure; steam generator pressure. These parameters are not completely independent. Pressurizer pressure low may be indicative of a pipe break LOCA, and steam generator pressure being low could be indicative of a stuck open PORV. Either of these, if valid, would be eventually accompanied by a high containment pressure indication, and this provides a form of self-checking should one of the indicators be misperceived or the wrong data source consulted. If the indications were completely independent and not correlated in any way, the appropriate thing to do would be to perform the assessment for each indication separately and add the HEPs. However, since the indications are correlated, the impact will be approximated by using a representative assessment using one of the parameters. These indications are all similar in the way they are trained on and in their HMI aspects.

Table A-1.4 CFM Selection Table – Critical Task 2

CRD Node	2 – Transfer to FR-H1	
Critical Task	Attempt to maintain SG levels between 22% and 50%, and failing to do so diagnose loss of heat sink	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	No	n/a. Response of this node is to a procedural step, not alarm.
AP-1: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable – key procedural step is Step 8 of ES-01.
SA-1: Data Misleading or Not Available	Yes	Applicable – AFW flow indicated when no flow to SG.
SA-2: Wrong Data Source Attended To	No	Flow indicator already incorrect; SG level continuously monitored in procedural step to control SG level.
SA-3: Critical Data Misperceived	No	Flow indicator already incorrect; SG level continuously monitored in procedural step to control SG level.
SA-4: Critical Data Dismissed/Discounted	No	No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	Even though this is a monitoring task it is not considered applicable. Two parameters are monitored continuously via the CSFST and checked via Step 8 of ES-01. This CFM is not applicable to flow because it is a misleading indication. This CFM is not applicable to SG level indication because the crew is in a procedural step to maintain level, which means it is being actively monitored. The only conclusion from the level dropping continuously is that there is a problem with feeding the SGs.
RP-1: Misinterpret Procedures	No	No viable alternative.
RP-2: Choose Inappropriate Strategy	No	No viable alternative.
E-1: Delay Implementation	No	Not an execution step.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	Not an execution step.
E-3: Fail to Initiate Execution	No	Not an execution step.
E-4: Fail to Correctly Execute Response (Simple Task)	No	Not an execution step.
E-5: Fail to Correctly Execute Response (Complex Task)	No	n/a. Not an execution step.

Table A.1.5 Assessment of Applicable CFMs for Node 2

SA-1 – Data Misleading		
PIF	Assessment	Justification
Alternate/Supplementary Source of Information	YES	SG level in this case is a supplementary source of data. Also, as later cues, core exit T/C temperature and AFWST level are also alternate sources of information.
Information Obviously Incorrect	NO	The flow indication reads a credible value and is not obviously failed (i.e., not pegged high or low).
Guidance to Seek Confirmatory Data	YES	The crew will be suspicious when they cannot restore the SG level even though flow is indicated, and it is standard practice to look at level in SGs to confirm flow. SG level indicator is given high credence, so will lead the operators to the right diagnosis.
Distraction	LOW HIGH	Long time frame scenario (a): Low distractions because all equipment lost is related to AFW and the crew is not trying to restore other functions. While they will have distractions by trying to restore MFW and the lost AFW trains, there is sufficient manpower and lots of time such that they can take their time in Step 8 to make the diagnosis of loss of heat sink. Short time frame scenario (b): High distraction because the indications are still not clear at this stage that the level is not dropping simply due to the fact that the AFW has not had time to recover level.
Manual Rx Trip (long time frame): Data Misleading Branch #5; Auto Rx Trip (short time frame): Data Misleading Branch #4;		
AP-1: Misread or Skip Critical Step in Procedure		
PIF	Assessment	Justification
Workload	LOW	Crew is focused on controlling level in SG; no other functions are challenged at this point.
Procedure	SIMPLE	Step 8 is a simple procedure, and the crew is very familiar with ES-01.
Compensatory Measures		This branch is not applicable when the procedures are simple and workload is low. However, this plant uses placekeeping aids (circle/slash) as standard practice.
Recovery Potential	YES	If skip RNO in Step 8a, Step 8c will cue crew to try to control NR level. Also STA is cognizant of NR level as part of monitoring CSFST and this provides the same information as procedural step. Because recovery for this CFM does not require breaking a mental model (i.e., not a lot of extra cognition time required) and because monitoring the CSFST is done in parallel with Step 8, this recovery is credited for both the short and long time frame scenarios.
Misread or Skip a Step Branch #14; Probability = negligible		

Table A.1.6 CFM Selection Table – Critical Task 3

CRD Node	3 - Begin Feed and Bleed	
Critical Task	Initiate and Execute feed and bleed	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	No	Response of this node is to a procedural step, not alarm.
AP-1: Misread or Skip Critical Step(s) in Procedure	No	Three redundant procedural cues (CIP, step 2 and step 9) would all have to be skipped, so this CFM, while in principle applicable, is screened out.
SA-1: Data Misleading or Not Available	No	Once in FR-H.1 the cues for starting B&F are not misleading
SA-2: Wrong Data Source Attended To	No	No other data source that it would be confused with since all the trains are being checked and tell the same story. If you confuse it with NR levels, they will be lower and the criteria will still be satisfied. Similarly, it was the low levels that led to transfer to FR-H1
SA-3: Critical Data Misperceived	Yes	The critical data to be read are SG WR levels; the PZR Pressure is assumed at this point to be within the normal range. It is the SG levels that will determine the need to go to F&B. However as noted above, it was the low SG levels that got the crew into RH-H1
SA-4: Critical Data Dismissed/Discounted	No	No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	Even though this is a monitoring task it is not considered applicable. Two parameters are monitored continuously via the CSFST and checked via Step 8 of ES-01. This CFM is not applicable to flow because it is a misleading indication. This CFM is not applicable to SG level indication because the crew is in a procedural step to maintain level, which means it is being actively monitored. The only conclusion from the level dropping continuously is that there is a problem with feeding the SGs.
RP-1: Misinterpret Procedures	No	Procedure not open to misinterpretation.
RP-2: Choose Inappropriate Strategy	No	No viable alternative.
E-1: Delay Implementation	Yes	Applicable – can delay start of B&F to try to restore AFW.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	CIP conditions are also most likely met at time the crew enters FR-H.1; in that case it would be a check or one-time assessment, not a monitoring activity. Teams that trip quickly and diagnose the LOHS quickly may not meet the B&F criteria when they enter FR-H.1, but in that case Step 2 and Step 9 will direct to start B&F and the criteria will be met by the time those steps are reached. In those steps, it is a check and not monitor, so this CFM is not applicable.
E-3: Fail to Initiate Execution	No	If there is no deliberate delay (see delay implementation), the initiation would be done immediately once the cue is received
E-4: Fail to Correctly Execute Response (Simple Task)	Yes	Steps 10-14 of FR-H.1.
E-5: Fail to Correctly Execute Response (Complex Task)	No	A simple task.

Table A.1.7 Assessment of applicable CFMs for Node 3

SA-3: Critical Data Misperceived		
PIF	Assessment	Justification
HSI/Environment	GOOD	The critical data to be read are SG WR Levels; the PZR Pressure is assumed at this point to be within the normal range. This is a primary indication that is frequently used through its full range, and furthermore, it was the low SG levels that got the crew into RH-H1
Workload	LOW	The workload is what is trained on and nominally expected for this action and this point in the scenario.
Training	GOOD	Checking Secondary Heat Sink is a task that is required in routine as well as emergency situations.
Recovery Potential	NO	Recovery potential is not evaluated or credited here.
Data Misperceived Branch #15;		
E-1: Delay Implementation		
PIF	Assessment	Justification
Reluctance and Viable Alternative	EXISTS	There are economic consequences of resorting to B&F, and a viable path in trying to restore the AFW.
Assessment of Time Margin	CORRECT	Operators are well trained on this scenario. The progression of this scenario is consistent with the expectations of crew. Crew is trained not to hesitate and strictly adhere to the procedure in that implementation is tied to a specific parameter value.
Additional Cues	YES	CSFTs will have the crew monitoring the core exit T/C temperatures and that will provide a strong additional cue that they can no longer delay B&F.
Delay Implementation Branch #4;		
E-4: Fail to Execute (simple task)		
PIF	Assessment	Justification
HSI	GOOD/ NOMINAL	Nominal HIS
Workload	LOW	Once in FR-H.1 that is their highest priority and where the attention will be – no completing functions to deal with.
Recovery Potential	YES NO	Long time frame: Immediate recovery via verification steps. Short time frame: Not enough time to re-do execution steps if fail the first time.
Manual Rx Trip (long time frame): Fail to Execute (Simple) Branch #8; Auto Rx Trip (short time frame): Fail to Execute (Simple) Branch #7;		

A.1.5 Final HEP and Discussion

Table A.1.8. Final HEP for long-time frame scenario (HFE 1a):

Node	CFM	HEP
1	Data Misperceived	negligible
2	Data Misleading	1E-2
2	Misread or Skip a Step	negligible
3	Data Misperceived	negligible
3	Delay Implementation	5E-3
3	Fail to Execute (Simple)	negligible
Total		1.5E-2

Table A.1.9. Final HEP for short-time frame scenario (HFE 1b):

Node	CFM	HEP
2	Data Misleading	1E-1
2	Misread or Skip a Step	negligible
3	Data Misperceived	negligible
3	Delay Implementation	5E-3
3	Fail to Execute (Simple)	1E-4
Total		1.1 E-1

This illustrates that the method is capable of making a distinction between the long and short time frame results. In this example, this distinction is primarily a result of the evaluation of the PIF workload in Node 2. This PIF is a surrogate for distraction, and the distraction in this case is caused by the fact that the plant has not settled into a state in which the lack of flow is easily detectable in the time available. In the long time frame scenario, if that was extended to be a very long time frame (i.e., > an hour) then an extra recovery factor may be applied to credit the TSC helping to break the mental model and diagnose the scenario. This extra level of recovery is discussed in Section 5.15.

A.2 Scenario 2: Loss of RCP Sealwater

This HFE was adapted from the NRC/Halden US Experimental Study HFE 2A. In the actual study, simulator runs showed that the HFE was not feasible due to the time available being less than the time required to perform all necessary actions (i.e., trip RCPs and start PDP). For this example, the time window was modified from 7-9 minutes to 13 minutes so that the action could be considered feasible and evaluated using IDHEAS.

A.2.1 PRA Scenario Description, Expected Operator Response and HFE Definition

PRA Scenario: A Westinghouse PWR is operating at power with the following equipment out of service:

- CCW train B out of service for maintenance
- AFW train B unavailable
- Diesel Generator B out of service for maintenance
- Charging pump A operating, pump B in standby.

All participating crew members are in the control room (Shift Manager, Unit Supervisor, Shift Technical Advisor and two Reactor Operators), and the plant is operating at 100%.

A distribution panel fails, with the consequential failure of the controlling channels for:

- A and B SGs.
- PZR level control
- Rod control
- Nuclear Instrumentation (NIS)
- PZR pressure control

The crew needs to take the equipment above in manual control, in particular they need to take manual control of the feedwater flow to SG A and B. However, the feedwater regulator valve on SG A cannot be operated manually and remains fully open, feeding the SG. If the crew does not trip the reactor, there will be an automatic turbine trip on high SG level (87%), which causes a reactor trip. In this scenario, the reactor trips on high SG level. AFW successfully starts as required.

To complicate things further, on Rx trip, Bus E1C will have bus lockout due to a bus fault. (The busbar is de-energized and the DG breaker cannot be closed.) CCW pump 1A breaker will trip due to a failed, seized shaft. Thus there are no CCW pumps in service, and the running charging pump trips. Furthermore, even if charging pump were to be started, it will trip 2 minutes after reactor trip. The C charging pump is de-energized.

The scenario leads to a complete loss of RCP cooling. RCP seal cooling needs to be restored in a timely manner to prevent a seal LOCA from occurring.

For PRA perspective the event tree in which the response occurs is portrayed below, with the relevant accident sequence indicated in red.

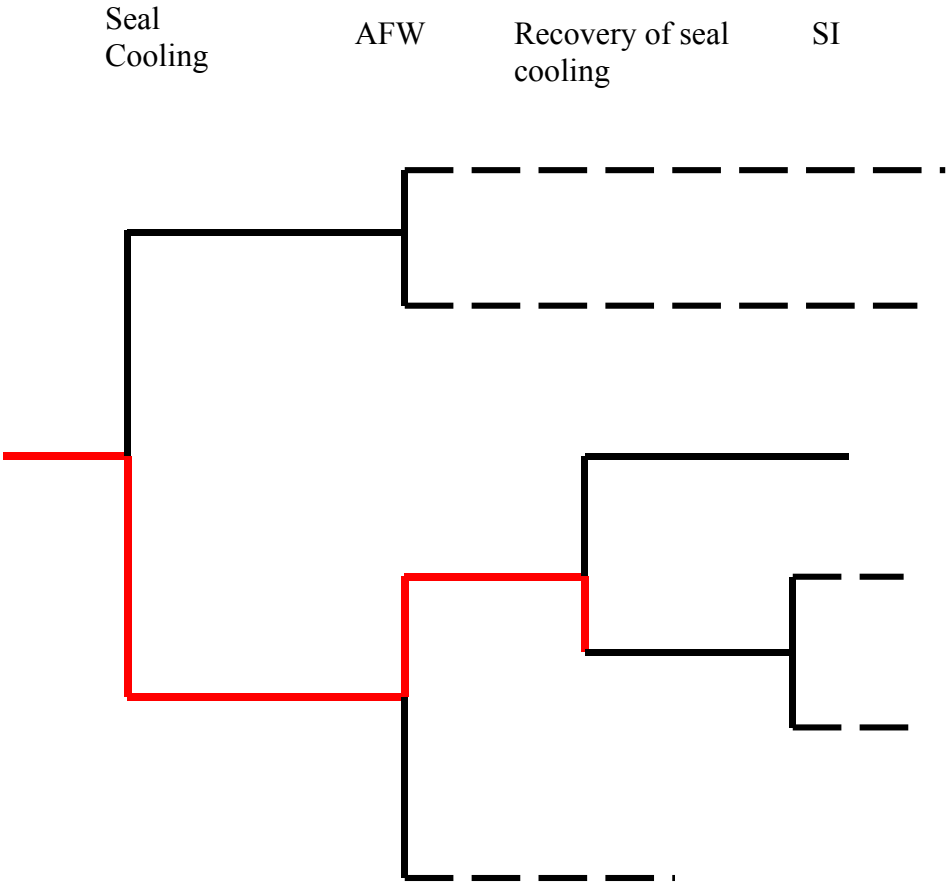


Figure A.2.1: Representative Event Tree

Expected response: Based on a review of the applicable procedures, the crew is directed to trip the RCPs after the loss of CCW and start a PDP to provide seal injection before seal water inlet or lower seal water bearing temperatures are greater than 230 degrees to avoid potential (not necessarily immediate) RCP seal LOCA. These are the necessary actions to prevent a seal LOCA.

HFE Definition: Failure of the crews to trip the RCPs and start the Positive Displacement Pump (PDP) to prevent RCP seal LOCA.

A.2.2 Crew Response Diagram (CRD) and Task Analysis

The applicable procedures were reviewed to identify the procedural guidance to trip the RCPs and start the PDP.

Reactor trip has occurred, therefore the operators will immediately enter E-0 (Represented as Node 0: Reactor trip and enter into E-0 (assumed success)), and perform the first four memorized steps.

At step 4 in E-0, they are asked to verify that SI is not required, and since it is not, the correct response is to transfer ES-01, and also start monitoring the Critical Safety Function Status Trees (CSFSTs). (Node 1: Enter ES-01)

ES-01 steps 1-5 are verifications of system/plant status. Step 6 is the critical step in ES-01 since it provides the guidance for starting the PDP.

Step 6:

b) Verify charging. There is no charging pump available, so the correct response is to go to the RNO column. The instruction for RNO b. 1), (no charging pump available) directs the crew to go to RNO for step 6.c.3
The RNO for 6.c.3 is the following:
3) IF a charging pump is not running, THEN:
a) PERFORM the following:
1) CHECK seal water inlet and lower seal water bearing temperatures LESS THAN 230˚F for each RCP. (Plant computer RC-010)
2) IF seal water inlet OR lower seal water bearing temperatures GREATER THAN OR EQUAL TO 230˚F THEN DO NOT establish seal injection to that RCP. GO TO Step 6.d.
b) ENSURE seal injection isolation valves open for applicable RCPs.
c) ENSURE PDP recirculation valve is 100% open.
d) START the PDP.
e) MONITOR seal water inlet and lower seal water bearing temperatures. (Plant computer display
RC-010)
f) Slowly CLOSE the PDP recirculation valve to establish a 1˚F/min. cooldown rate on seal water inlet and lower seal water bearing temperatures.
g) ESTABLISH normal seal injection flow of between 6 and 13 gpm.

This is the procedural direction for starting the PDP. (Node 4: Start PDP)

NOTE: There is no direction in ES-01 to stop the RCPs.

However, there will be indications of loss of seal cooling (Annunciators for loss of CCW and loss of seal injection) and the response to these annunciators is to enter RC-0002 (Reactor Coolant Pump Off Normal Procedure). (Node 2: Enter RC-0002)

Cues and Indications	
Initial Cue	CCW fails The failure of the CCW can be diagnosed using the following annunciator lamp box cues: CCW PUMP 1A(2A) TRIP CCW HX 1A(2A) OUTL TEMP HI CCW HX 1A(2A) OUTL PRESS LO
Recovery Cue	RCP 1A(2A) THERM BAR CCW FLOW/TEMP/TRBL RCP 1B(2B) THERM BAR CCW FLOW/TEMP/TRBL RCP 1C(2C) THERM BAR CCW FLOW/TEMP/TRBL RCP 1D(2D) THERM BAR CCW FLOW/TEMP/TRBL
Additional Cues	1. CP 1A(2A) SEAL WTR INJ FLOW LO RCP 1A(2A) NO 1 SEAL DP LO RCP 1B(2B) SEAL WTR INJ FLOW LO RCP 1B(2B) NO 1 SEAL DP LO RCP 1C(2C) SEAL WTR INJ FLOW LO RCP 1C(2C) NO 1 SEAL DP LO RCP 1D(2D) SEAL WTR INJ FLOW LO
Cue Comments	The initial cues will occur when the CCW pump trips. In addition, the recovery cues will appear as the CCW heats up due to no low flow.

Figure A.2.2 Cues for Loss of Seal Cooling

Step 3 of RC-0002 instructs the operators to CHECK RCP thermal barrier CCW flow and Seal Injection flow, neither of which will be adequate, leading to the RNO column. The RNO a2

directs operators to trip RCPs within 1 minute of loss of cooling, continue in procedure as time permits (all checks and attempts to restore), and perform Addendum 1 to restore normal RCP seal cooling. (Node 3: Trip RCPs)

In Addendum 1 at step 11, since no charging pump is running, the crew is directed to the RNO for which step g states: if seal temperature less than 230˚F, start PDP. The intervening steps in Addendum 1are related to trying to re-establish cooling via CCW or CCP or checking status of various components.

Thus there is one procedural direction to trip the RCPs (RC-0002) and two instructions to start the PDP (from ES-01 Step 6 and RC-0002, Addendum 1 Step 11).

Based on timing considerations (see Section A.2.3) the following CRD is constructed.

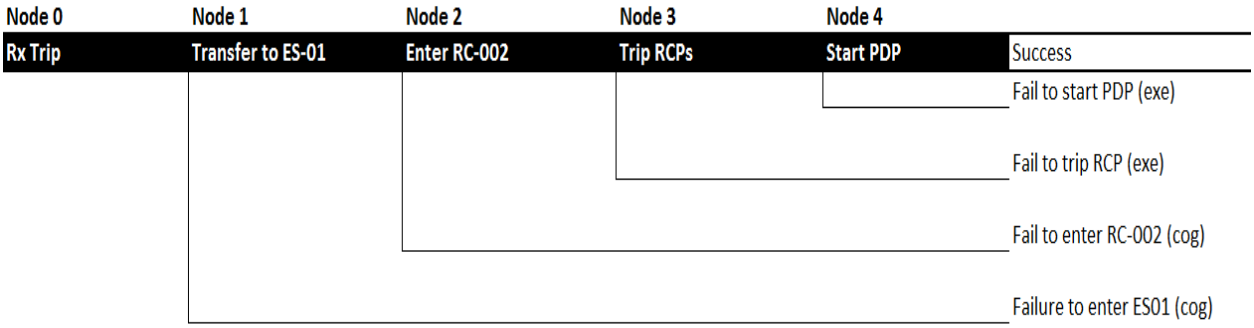


Figure A.2.3 CRD for Failure to Restore Seal Cooling

Node 0: Reactor trip and enter into E-0 (assumed success)

Node 1: Enter ES-01

- ES-01 is the only feasible path to initiation of PDP (RC-0002 takes too long)
- Starting the PDP is not a memorized or familiar response

Node 2: Enter RC-0002

- Only procedural directive to trip RCPs
- However, tripping RCPs is generally recognized as important

Node 3: Trip RCPs

- If RCPs are not tripped, won't get to step in ES-01 to start PDP in time
- From Step 3 in RC-0002

Node 4: Start PDP

- From Step 6 in ES-01

Failure at any of these nodes results in an RCP seal LOCA. The nodes are defined in the following table where the activities required of the crew for success are identified. (This is an essential precursor to choosing the appropriate CFMs.)

Table A.2.1 Task Analysis Table

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information
1	1	At step 4 of E-0, check indications to determine whether SI is required	Locate the appropriate indicator(s). Read the numerical value(s) correctly. Understand that the indication(s) is(are) not in the normal range. Correctly interpret the procedural directive to transfer to ES-01	The SI indications are not lit. RNO for step 4 reads: a. PERFORM the following: 1) CHECK if SI is required: o Pressurizer pressure – LESS THAN OR EQUAL TO 1857 PSIG AND NOT BLOCKED. OR o Containment pressure - GREATER THAN OR EQUAL TO 3 PSIG. OR o Any SG pressure - LESS THAN OR EQUAL TO 735 PSIG AND NOT BLOCKED. OR o As directed by US/SS. 2) IF SI is required, THEN manually ACTUATE. 3) IF SI is NOT required, THEN GO TO ES-01, REACTOR TRIP RESPONSE, Step 1 AND MONITOR Critical Safety Functions.
2	2	Enter RC-0002	Respond to multiple alarms	There are several alarms related to CCW and seal water injection flow.
3	3	Trip the RCPs (Step 3, RNO a2).	Simple execution	
4	4	Start PDP at step 6c of ES-01	Complex execution	See discussion above. Starting the PDP involves a number of steps that include monitoring plant response.

A.2.3 Timeline

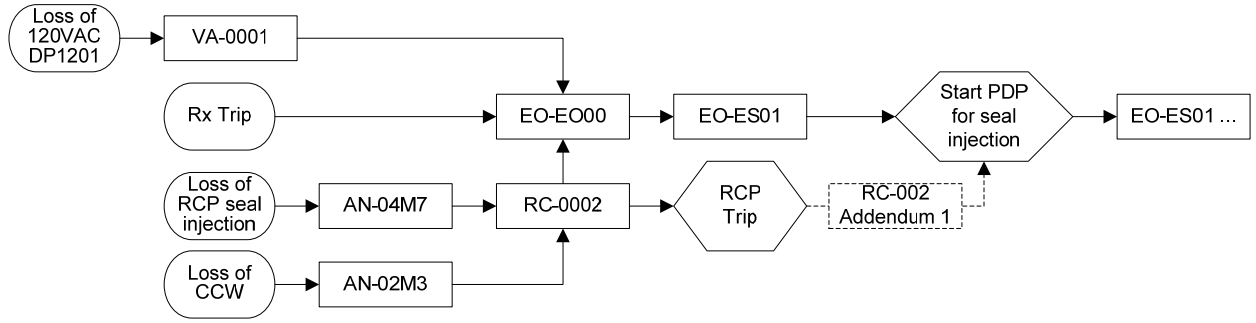


Figure A.2.4. Map of Procedural Steps

On discussion with plant staff the following information was obtained. Because of the distractions due to the loss of 120VAC DP 1201, it will take the operators 4-7 minutes to diagnose and stop the RCPs. Despite the distractions due to the loss of Distribution Panel, the

operators are expected to correctly diagnose the scenario and time becomes the most influential factor on the crew's success. Any actions taken to address the RCP (either knowledge based or via RC-002) will occur in parallel with E-0/ES-01.

The time critical action, in this case, becomes starting the Positive Displacement Pump (PDP), which is part of the success criteria for the HFE. Once complete with step 4 of E-0, the crew will proceed through EOP ES-01. Step 6c of ES-01 will cue the operator to check if a charging pump is NOT running and, if so, start the PDP. When the distribution panel is lost, they lose several key controlling channels, most notably for SGs A and B and the pressurizer level control. On the loss of pressurizer level control operators will lose critical time when they have to complete the RNO portion of step 6.a. Therefore, it is estimated to take at least 11 minutes from Rx trip to get to step 6c and start the PDP. Alternatively, if the crew gets into RC-002, step 3 directs the operators to Addendum 1, and step 11 of Addendum 1 directs the operators to start the PDP; this procedural route is estimated to take 12-15 minutes from reactor trip. Starting the PDP immediately is not part of the operator training (memorized action) the way stopping the RCPs was.

Another key factor that would affect the crew's behavior would be the workload this scenario presents. Between the distribution panel failure and the reactor trip, the crew will have to work through multiple procedures in tandem to properly diagnose the cues and resolve the situation. Besides the issues with timing and workload, it is expect the remaining conditions that contribute to operator behavior to be optimal including the environmental conditions and the complexity of the task.

In summary:

- Both procedures would be in use simultaneously
- Entry into ES-01 will take about 1 minute
- Cue to stop RCPs (RC-0002 step 3 and CIP) reached in 4-7 minutes
- Estimate 10-12 minutes to get to Step 6c of EOP ES-01 and start the PDP
- Estimate 13-15 minutes to start PDP via RC-0002
- It is estimated to take at least 11 minutes from Rx trip to get to step 6c and start the PDP
- Alternatively, this procedural route to start the PDP via RC-0002, step 3 and step 11 of Addendum is estimated to take12-15 minutes from reactor trip.
- Starting the PDP immediately is not part of the operator training (memorized action)
- However, stopping the RCPs is a well-trained response.

Based on an analysis of seal heat up, the time window is 13 minutes if the RCPs are tripped in a timely manner. Based on a review of the time required (see below, time required is 11 minutes) starting the PPD via ES-01 is determined to be feasible, but time critical. However, if the RCPs are not tripped in a timely manner, the heat up time is shorter and even this path becomes infeasible. Starting the PDP via the RC-0002 is either marginally or not feasible.

The crew response tree (CRD) for this HFE is as follows:

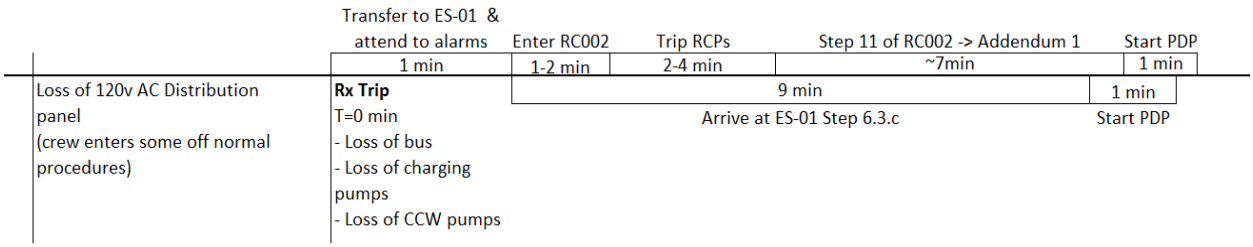


Figure A.2.5. Timeline for Loss of Sealwater

A.2.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees (DTs)

Node 0: Rx Trip (Auto or manual)

Not Evaluated. The plant will trip either automatically or by operator action. This affects the time available to perform the responses and should be evaluated separately for the two cases.

Table A.2.2 CFM selection table – Critical Task 1

CRD Node	1 – Transfer to ES-01	
Critical Task	1 – Check indications to determine whether SI is required. Note: Since there are several indications that need to be checked, SA-2 and SA-3 apply to the activity associated with each of these indication checks.	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	No	n/a. Response of this node is to a procedural step, not alarm.
AP-1: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable in principle (Step 4 of E-0). However, this is one of the immediate actions on a reactor trip, and as such it can be screened out.
SA-1: Data Misleading or Not Available	No	n/a. For this PRA scenario there is no misleading data.
SA-2: Wrong Data Source Attended To	Yes	Multiple data sources (see note above)
SA-3: Critical Data Misperceived	Yes	Multiple data sources (see note above).
SA-4: Critical Data Dismissed/Discounted	No	n/a. No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	n/a. Not a monitoring task.
RP-1: Misinterpret Procedures	No	n/a. No viable alternative.
RP-2: Choose Inappropriate Strategy	No	n/a. No viable alternative.
E-1: Delay Implementation	No	n/a. Not an execution step.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	n/a. Not a monitoring task.
E-3: Fail to Initiate Execution	No	n/a. Not an execution step.
E-4: Fail to Correctly Execute Response (Simple Task)	No	n/a. Not an execution step.
E-5: Fail to Correctly Execute Response (Complex Task)	No	n/a. Not an execution step.

This step in the procedure is a memorized step in the procedure and the expected scenario would be one for which there is no need for SI. The CFMs SA-2 and SA-3 need to be assessed for each of the critical parameters: pressurizer pressure; containment pressure; steam generator pressure. These parameters are not completely independent. Pressurizer pressure low may be indicative of a pipe break LOCA, and steam generator pressure being low could be indicative of a stuck open PORV. Either of these, if valid, would be eventually accompanied by a high containment pressure indication, and this provides a form of self-checking should one of the indicators be misperceived or the wrong data source consulted. If the indications were completely independent and not correlated in any way, the appropriate thing to do would be to perform the assessment for each indication separately and add the HEPs. However, since the indications are correlated, the impact will be approximated by using a representative assessment using one of the parameters. These indications are all similar in the way they are trained on and in their HMI aspects.

Table A.2.3 Assessment of CFMs applicable to Node 1

SA-2: Wrong Data Source Attended to		
PSF	Assessment	Justification
HSI	GOOD	Parameter is an important one, therefore HSI is presumed not to be poor
Workload	HIGH	This is a very complex scenario with multiple failures leading to a high cognitive demand. NOTE: However, since this occurs immediately after reactor trip and determining whether SI is needed is a priority, the crew is unlikely to be distracted from this activity. Therefore the assignment of High is possibly conservative, and this is flagged as a source if uncertainty.
Familiarity with Data Source	GOOD	
Recovery Potential	NO	If they don't get into ES-01 there is insufficient time margin to rely on transfer from later steps in E-0
Crew Failure Scenario #		11

SA-3: Critical Data Misperceived		
PIF	Assessment	Justification
HSI/Environment	GOOD	Parameter is an important one, therefore HSI is presumed not to be poor.
Workload	HIGH	This is a very complex scenario with multiple failures leading to a high cognitive demand. NOTE: However, since this occurs immediately after reactor trip and determining whether SI is needed is a priority, the crew is unlikely to be distracted from this activity. Therefore the assignment of High is possibly conservative, and this is flagged as a source if uncertainty.
Training	GOOD	Training on E-0 is good
Recovery Potential	NO	There is no time margin sufficient to allow for procedural recovery
Crew Failure Scenario #		11

Table A.2.4 CFM selection table – Critical Task 2

CRD Node	2 - Enter RC-0002	
Critical Task	2 – Respond to multiple alarms	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	Yes	This CFM covers all phases of the required response, therefore, by definition all other CFMs are not applicable.
AP-1: Misread or Skip Critical Step(s) in Procedure	No	n/a.
SA-1: Data Misleading or Not Available	No	n/a.
SA-2: Wrong Data Source Attended To	No	n/a.
SA-3: Critical Data Misperceived	No	n/a.
SA-4: Critical Data Dismissed/Discounted	No	n/a.
SA-5: Premature Termination of Critical Data Collection	No	n/a.
RP-1: Misinterpret Procedures	No	n/a.
RP-2: Choose Inappropriate Strategy	No	n/a.
E-1: Delay Implementation	No	n/a.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	n/a.
E-3: Fail to Initiate Execution	No	n/a.
E-4: Fail to Correctly Execute Response (Simple Task)	No	n/a.
E-5: Fail to Correctly Execute Response (Complex Task)	No	n/a.

Table A.2.5 Assessment of CFM applicable to Critical Task 2

AR: Key Alarm Not Attended To		
PSF	Assessment	Justification
Cognitive Workload/Distraction	HIGH	High distraction because of the Reactor trip and other failures not related to loss of CCW. In the short time frame, failure of a distribution panel is considered a major distracter because there are multiple alarms going that need to be dealt with.
HSI	NOMINAL/GOOD	The cues are lamp boxes on one panel. The HSI is nominal.
Perceived Urgency/Significance	HIGH	Alarm pattern is understood as being critical and must be dealt with immediately (importance of seal cooling understood). This is a scenario emphasized by training.
Crew Failure Scenario #		4

Table A.2.6 CFM selection table – Critical Task 3

CRD Node	3 - Trip RCPs	
Critical Task	3 – Trip RCPs	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	No	n/a. Response of this node is to a procedural step, not alarm.
AP-1: Misread or Skip Critical Step(s) in Procedure	Yes	Step 3 is the relevant step.
SA-1: Data Misleading or Not Available	No	n/a. No misleading data.
SA-2: Wrong Data Source Attended To	No	n/a. In principle, this could be considered applicable since there are several parameters to be checked to determine that there is no seal cooling, including seal injection flow and CCW flow to RCP thermal barrier, but since alarms related to these parameters have already been attended to get into RC-0002, the likelihood of a failure from these CFMs is considered negligible.
SA-3: Critical Data Misperceived	No	n/a. See SA-2.
SA-4: Critical Data Dismissed/Discounted	No	n/a. No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	n/a. Not a monitoring task.
RP-1: Misinterpret Procedures	No	n/a. Procedure unambiguous.
RP-2: Choose Inappropriate Strategy	No	n/a. No viable alternative.
E-1: Delay Implementation	No	n/a. Procedural direction to implement as fast as possible and no other viable alternative. In principle this could be considered applicable, but operators are trained to trip RCPs immediately whenever required to do so.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	n/a. Not a monitoring task.
E-3: Fail to Initiate Execution	Yes	Applicable – procedural direction is to trip RCPs
E-4: Fail to Correctly Execute Response (Simple Task)	Yes	This is a simple execution step.
E-5: Fail to Correctly Execute Response (Complex Task)	No	n/a. (by exclusion).

Table A.2.7 Assessment of CFMs applicable to Critical Task 3

AP-2: Misread or Skip Critical Step(s) in Procedure		
PSF	Assessment	Justification
Workload	LOW	While the general workload is high for the crew, low workload is applicable here because this relates to the workload of the operator who is dealing with RC002 only and therefore focused on the task at hand without additional workload or distracters.
Procedure	SIMPLE	Simple procedure with normal formatting.
Compensatory Factors	N/A	However, placekeeping aids standard practice (circle/slash) even for off normal procedure.
Recovery Potential	NO	
Crew Failure Scenario #		13

E-3: Fail to Initiate Execution		
PIF	Assessment	Justification
Immediacy	YES	The instruction is clear to stop the RCPs within 1 minute, and the operators are well aware of the need to trip RCPs.
Workload	N/A	
Recovery Potential	N/A	
Crew Failure Scenario #		5

E-4: Fail to Correctly Execute Response (Simple Task)		
PSF	Assessment	Justification
HSI	NOMINAL/ GOOD	HSI is good/nominal in that the control is clear and follows the populational stereotype.
Workload	LOW	While the general workload is high for the crew, low workload is applicable here because this relates to the workload of the operator who is dealing with RC002 only and therefore focused on the task at hand without additional workload or distractors.
Recovery Potential	NO	No viable recovery path.
Crew Failure Scenario #		7

Table A.2.8 CFM selection table for Critical task 4

CRD Node	4 - Start PDP	
Critical Task	4 – Start PDP	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	No	n/a. Response of this node is to a procedural step, not alarm.
AP-1: Misread or Skip Critical Step(s) in Procedure	Yes	Step 6 of ES-01 is the relevant step.
SA-1: Data Misleading or Not Available	No	n/a. No misleading data.
SA-2: Wrong Data Source Attended To	No	This could be considered applicable in principle. The data sources are the seal lower bearing temperature and the seal water inlet temperature. However, the procedure directs the operators to a specific location in the plant computer. Since they know they are looking for temperatures the wrong data sources would need to be other temperature readings. Discussions with the operators indicated this was not a possibility.
SA-3: Critical Data Misperceived	Yes	In principle, this is applicable – the operators must correctly perceive that the charging pump is not running AND either of two indications of seal temperature are < 230 ˚. The former is assumed to be a given. If the temperature were assessed incorrectly as being above 230 ˚, they would bypass the start of the PDP.
SA-4: Critical Data Dismissed/Discounted	No	n/a. No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	n/a. Not a monitoring task.
RP-1: Misinterpret Procedures	No	n/a. Procedure unambiguous.
RP-2: Choose Inappropriate Strategy	No	n/a. No viable alternative.
E-1: Delay Implementation	No	In principle this is applicable. This should be a high priority task so there is no reason to delay. If the DT were applied the default (end-point 7) would apply.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	n/a. Not a monitoring task.
E-3: Fail to Initiate Execution	Yes	Applicable – procedural direction is to start PDP.
E-4: Fail to Correctly Execute Response (Simple Task)	No	This is a complex execution step.
E-5: Fail to Correctly Execute Response (Complex Task)	Yes	By definition this is treated as a complex execution step.

Table A.2.9 Assessment of CFMs applicable to Critical Task 4

AP-2: Misread or Skip Critical Step(s) in Procedure		
PSF	Assessment	Justification
Workload	HIGH	This procedural step is being directed by the US, who is also occupied by keeping situational awareness of the multiple alarm response and off-normal procedures in effect due to the lost distribution panel.
Procedure	SIMPLE	Simple procedure with normal formatting.
Compensatory Factors	PRESENT	Placekeeping aids standard practice (circle/slash).
Recovery Potential	NO	
Crew Failure Scenario #		7

SA-3: Critical Data Misperceived		
PSF	Assessment	Justification
HSI/Environment	NOMINAL	HSI and environment are nominal.
Workload	HIGH	This procedural step is being directed by the US, who is also occupied by keeping situational awareness of the multiple alarm response and off-normal procedures in effect due to the lost distribution panel.
Training	POOR	While not specifically trained on the time-critical importance of starting the PDP in this specific situation, the crew has generally good training on ES-01, including this step in the procedure. However, it is not clear that the RNO for Step 6 is trained on, so conservatively the POOR branch is taken.
Recovery Potential	NO	
Crew Failure Scenario #		9

E-3: Fail to Initiate Execution		
PIF	Assessment	Justification
Immediacy	YES	Given that they are aware they have no seal cooling, the crew will treat this as an immediate action
Workload	N/A	
Recovery Potential	N/A	
Crew Failure Scenario #		5

E-5: Fail to Correctly Execute Response (Complex Task)		
PIF	Assessment	Justification
Execution Straightforward	NO	Based on interviews conducted with operators, this is regarded by operators as a “tricky” control action
Training	POOR	Not a scenario that has been trained on to any significant degree.
Work Practices	POOR	Standard work practices (check-off for example) will not be a significant compensatory factor
Recovery Potential	NO	Recovery potential n/a for control actions.
Crew Failure Scenario #		1

A.2.5 Summary of analysis

This scenario is very complex and not one that is well practiced. There are significant distractions caused by the numerous failures that occur. This is reflected in the analysis by the choice of high workload for many of the CFMs. Furthermore, this is a time critical action; there is very little time margin so there is no opportunity for recovery based on additional procedural steps or additional cues.

Workload is a significant negative PIF for this HFE, primarily due to the very complex evolution of the scenario. Based on this assessment, the most significant contributors to the HEP are:

- Node 2 (fail to enter RC-0002). While there are multiple alarms and they are reinforcing in indicating loss of seal cooling, the numerous failures involved in the scenario would be a significant distractor which could lead to a delayed response.
- Node 4 (failure to start the PDP). The operators considered this a very complex response, and one that is not practiced. Therefore, failure to execute is identified as a significant contributor to the HEP.

Table A.2.10 Summary of contributors to HFE

CRD Node #	Critical Task #	CFM	Crew Failure Scenario #	HEP
1	1	AP-2: This is considered to be a negligible contributor to the HEP, since this is one of the memorized actions	N/A	
		SA-2: Wrong data source attended to	11	
		SA-3: Critical data misperceived	11	
2	2	AP-1: Key alarm not attended to	4	
3	3	AP-2: Misread or Skip Critical Step(s) in Procedure	13	
		E-3: Fail to Initiate Execution	5	
		E-4: Fail to Correctly Execute Response (Simple Task)	7	
4	4	AP-2: Misread or Skip Critical Step(s) in Procedure	7	
		SA-3: Critical Data Misperceived	9	
		E-3: Fail to Initiate Execution	5	
		E-5: Fail to Correctly Execute Response (Complex Task)	1	
Total HEP:				

Table A.2.11: Final HEP for HFE 2

Node	CFM	HEP
1	Data Misperceived	1E-4
2	Key Alarm	5E-2
3	Misread or Skip a Step	5E-5
3	Fail to Execute (Simple)	1E-5
4	Data Misperceived	1E-4
4	Misread or Skip a Step	5E-5
4	Fail to Execute (Complex)	1E-1
Total		1.5E-1

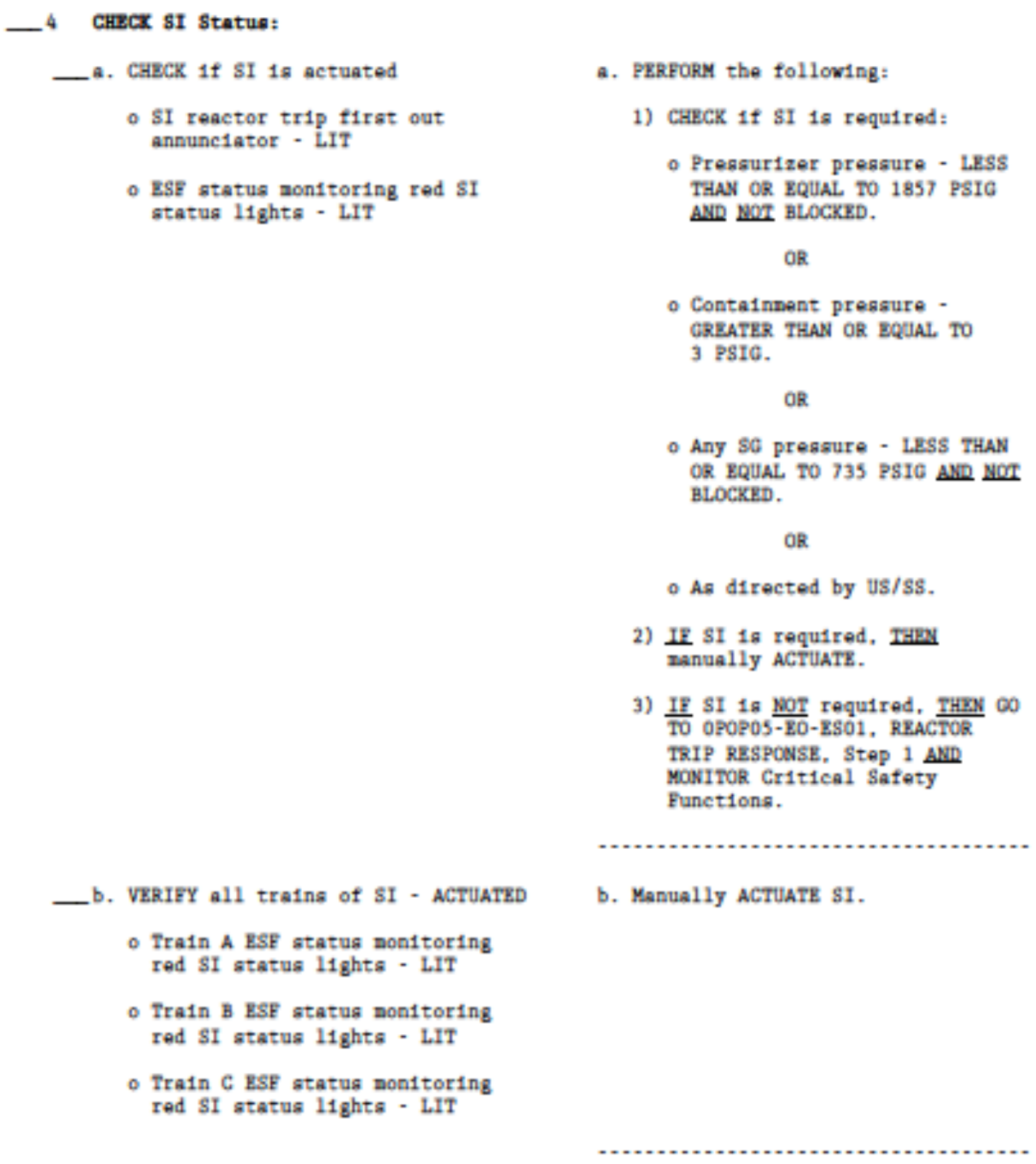
HEP = 1.5E-1. This HEP is consistent with simulator observations and operator interviews. The two dominant failure mechanisms were 1) fail to start PDP (fail to execute complex action; 1E-1) and 2) failure to enter RC002 (key alarm response; 5E-2). While there is no simulator data on the failure to start the PDP, operator interviews indicated that it would be a very difficult control action with low anticipated success rate. For failure to enter RC002, in the simulator observation 1 of 4 crews failed to get into RC002 due to the high level of distractions.

Through this example, two insights into the use of IDHEAS should be mentioned regarding 1) building the CRT and 2) the definition of "critical piece of data".

In this example there were several ways for the crew to stop the RCPs and start the PDP, and, therefore, several ways to possibly construct the CRD. The analysis team picked this particular construction because it was the most likely path for the operators and it clearly laid out the critical steps for success. In constructing the CRD the analysis team went through several iterations, and confirmed that while the different tree structures may have had a slightly different CFM mix, they yielded the same risk insights (same driving CFMs and PIFs). If they did not yield the same risk insights the team would have to understand why one path was better than the other and then cycle back with the operators or training and investigate the response further or use the more conservative HEP. The fact that two procedural paths may exist and one is potentially more successful that the other is in itself a risk insight. While variation in the CRDs may be a source of analyst-to-analyst variability, it is a documented reflection of the variability in the analysts' understanding of the progression of the scenario and critical steps. Therefore, if there is a difference in the resultant HEPs, it can be traced back ultimately to the assumptions driving the choice of the CFMs.

The second insight is regarding what is considered a "critical piece of data" when there are multiple indicators in a procedural step. Several CFMs are applied to the perception and interpretation of "critical" data. Whether or not a piece of data is critical depends upon the context of the scenario and whether misperceiving or misinterpreting it will lead the crew off the success path. Take for example Steps 4.a.1 in the RNO column of E-0 in Figure A.2.6 below. There are three cues, and if ANY of them is INCORRECTLY understood then that will lead the crew to actuate SI and continue through E-0 (off the success path, which would be to transfer to ES-01 in 4.a.3). Therefore, in this example, the cues for 4.a.1 are considered "critical data" and the "critical data misperceived" CFM is applicable in this case. Alternatively, the entry criteria for RC002 (Figure A.2.7) has no "critical data". There are several parameters that need to be checked in step 3, ANY of which being CORRECT will lead the crew down the success path (i.e., to the RNO column to stop the RCPs. In this case, if any one parameter is misperceived or misinterpreted, it does not change the outcome (i.e., if the first piece of data is correctly perceived it will get to the correct path, if it is misperceived the operator will be prompted to check the next parameter (and so forth), which will cue them correctly for action). Therefore, the "Critical Data Misperceived" CFM was not considered applicable to this node.

Figure A.2.6. Extract of Step 4 of E0



___4 **CHECK SI Status:**

___a. CHECK if SI is actuated

- o SI reactor trip first out annunciator - LIT
- o ESF status monitoring red SI status lights - LIT

a. PERFORM the following:

1) CHECK if SI is required:

- o Pressurizer pressure - LESS THAN OR EQUAL TO 1857 PSIG AND NOT BLOCKED.

OR

- o Containment pressure - GREATER THAN OR EQUAL TO 3 PSIG.

OR

- o Any SG pressure - LESS THAN OR EQUAL TO 735 PSIG AND NOT BLOCKED.

OR

- o As directed by US/SS.

2) IF SI is required, THEN manually ACTUATE.

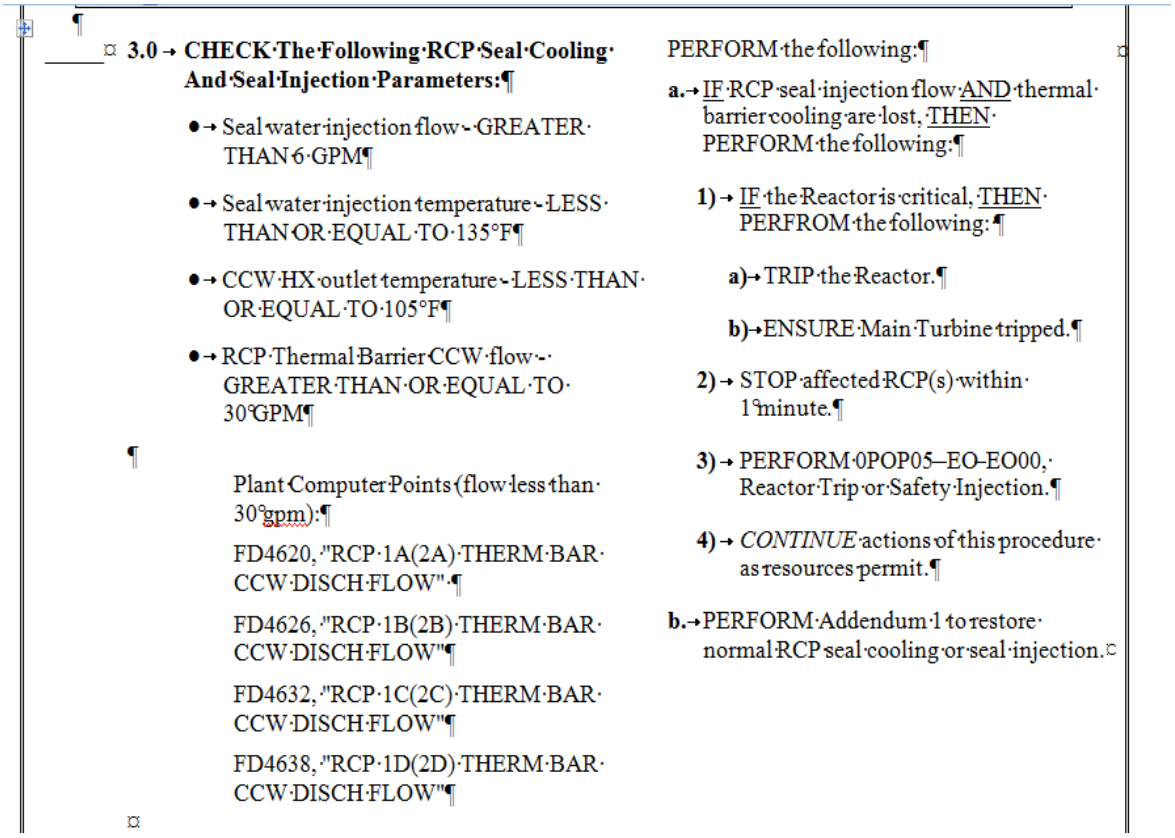
3) IF SI is NOT required, THEN GO TO 0POP05-EO-ES01, REACTOR TRIP RESPONSE, Step 1 AND MONITOR Critical Safety Functions.

___b. VERIFY all trains of SI - ACTUATED

- o Train A ESF status monitoring red SI status lights - LIT
- o Train B ESF status monitoring red SI status lights - LIT
- o Train C ESF status monitoring red SI status lights - LIT

b. Manually ACTUATE SI.

Figure A.2.7. Excerpt of Step 3 of RC-002



3.0 CHECK The Following RCP Seal Cooling And Seal Injection Parameters:

- Seal water injection flow - GREATER THAN 6 GPM
- Seal water injection temperature - LESS THAN OR EQUAL TO 135°F
- CCW HX outlet temperature - LESS THAN OR EQUAL TO 105°F
- RCP Thermal Barrier CCW flow - GREATER THAN OR EQUAL TO 30 GPM

Plant Computer Points (flow less than 30 gpm):

FD4620, "RCP 1A(2A) THERM BAR CCW DISCH FLOW"

FD4626, "RCP 1B(2B) THERM BAR CCW DISCH FLOW"

FD4632, "RCP 1C(2C) THERM BAR CCW DISCH FLOW"

FD4638, "RCP 1D(2D) THERM BAR CCW DISCH FLOW"

PERFORM the following:

a. IF RCP seal injection flow AND thermal barrier cooling are lost, THEN PERFORM the following:

1) IF the Reactor is critical, THEN PERFROM the following:

a) TRIP the Reactor.

b) ENSURE Main Turbine tripped.

2) STOP affected RCP(s) within 1 minute.

3) PERFORM 0POP05–EO-EO00, Reactor Trip or Safety Injection.

4) *CONTINUE* actions of this procedure as resources permit.

b. PERFORM Addendum 1 to restore normal RCP seal cooling or seal injection.

A.3 Scenario 3 – Fail to Cooldown and Depressurize Following a Small LOCA

A.3.1 PRA Scenario Description, Expected Operator Response and HFE Definition

PRA Scenario: The plant is a 2 loop Westinghouse PWR, operating at 100% power with no out of service safe shutdown equipment. The initiating event is a pipe break causing a small LOCA, such that the CVCS cannot maintain RCS inventory. An automatic reactor trip occurs and SI initiates on low pressurizer pressure. SI takes suction from the RWST. The break is not large enough to neither remove decay heat nor depressurize the primary system rapidly. Therefore, secondary side heat removal is needed.

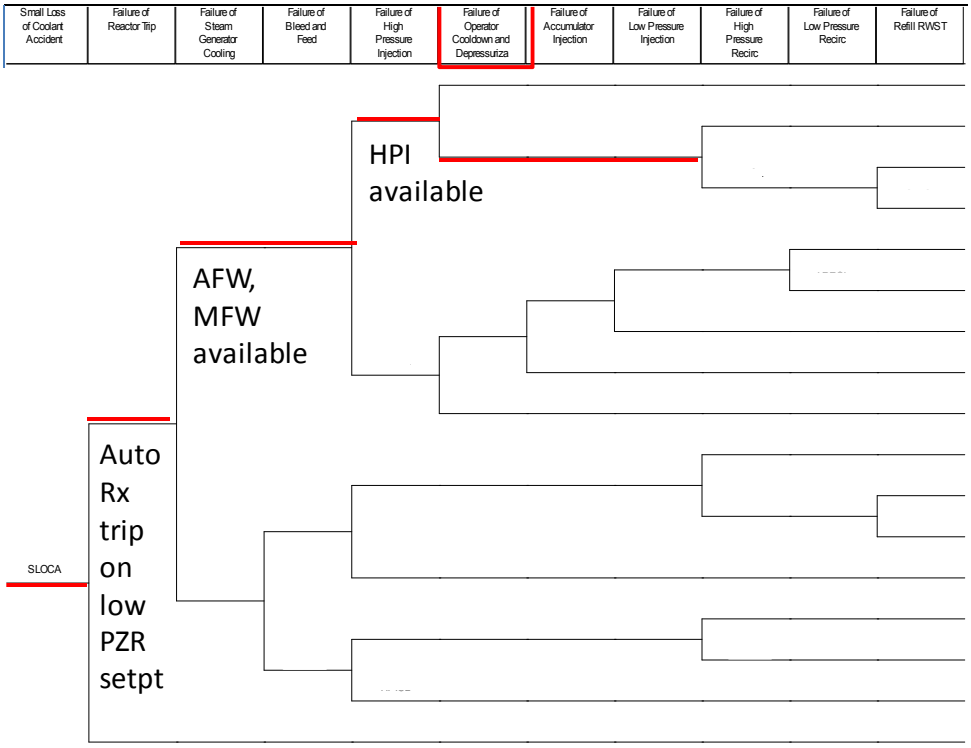
At the beginning of the scenario the Shift Technical Advisor is not in the control room. He or she will arrive 5 minutes after being called. The other participating crew members are in the control room (SM, US, 2 ROs). The procedures instruct operators to cooldown and depressurize the primary system to establish decay heat removal using the RHR system and to terminate the leak. If this is not successful, the only recourse is to continue using the SI system taking suction from the RWST. However, the RWST is a finite source, so at some point, the operators will have to transfer to sump recirculation, or begin refilling the RWST.

Expected Operator Response: The required operator response is to cooldown and depressurize the RCS to allow initiation of the RHR function. The “cue” is EOP E-1 Step 22 which directs the operators to begin cooldown and depressurization if the RCS pressure is

greater than 270psig (which T/H calculations have shown to be the case). If the response is not completed before the RWST is depleted, the operators would need to go to sump recirculation to prevent core damage. Success is defined as achieving RHR conditions before RWST is depleted.

Figure A.3.1 shows the small LOCA event tree that includes the operator action to cooldown and depressurize the reactor.

Figure A.3.1 Small LOCA Event Tree



HFE Definition: Functionally the HFE is defined as operators fail to achieve RHR conditions before RWST is depleted.

A.3.2 Crew Response Diagram (CRD) and Task Analysis

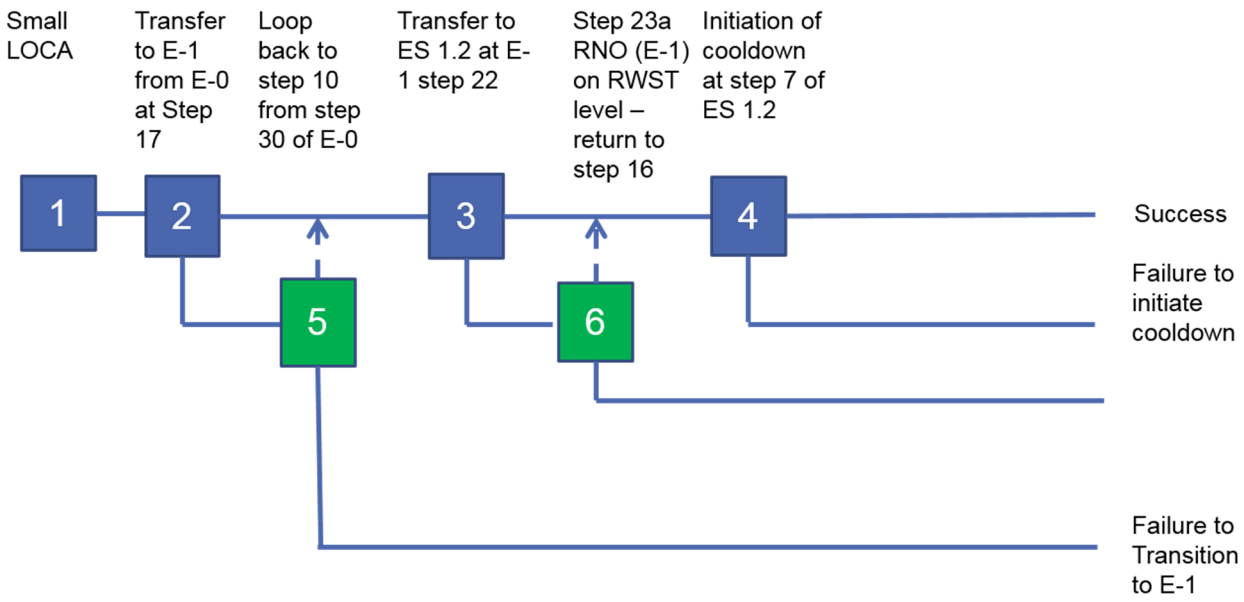


Figure A.3.2 CRD for the HFE Failure to Cooldown and Depressurize

The procedural path represented by this CRD is discussed below.

Node 1: Successful recognition of reactor trip and enter E-0 (assumed success)

Information only. The Small LOCA leads to Reactor Trip based on low pressurizer pressure, which causes operators to enter procedure E-0 for Reactor Trip or Safety Injection. For this and all other procedures that are implemented, the operators would check the Fold Out Page for continuous use to identify whether or not any of the specified conditions apply. In the case of E-0, they do not, so the operators proceed to E-0 step 1 and perform the immediate, memorized actions (Steps 1-4), continuing on through to step 17. There is no way for the operators to be diverted off the success path in the interim steps between 4 and 17.

The operators would need to verify SI is automatically actuated per Step 5 of E-0, which states:

ENSURE Automatic Actions Using ATTACHMENT A, SI AUTOMATIC ACTION VERIFICATION, While Continuing With This Procedure

They would therefore need to complete Attachment A of E-0 before transferring to E-1, however, in this scenario, SI is considered to be actuated normally. Still, the review of Attachment A is addressed as part of the scenario timeline.

Node 2: Successful transfer to E-1 at Step 17 of E-0

At the point where they reach Step 17 in E-0, the operators would transition to procedure E-1 for Loss of Reactor or Secondary Coolant via the Response Not Obtained (RNO) for an intact RCS. There are four separate cues (17a through d) based on different containment parameters and none of them would be normal in this case. After completing Attachment A (essentially verifications and checks but no required response for this scenario), the operators transfer to EOP E-1, “Loss of Reactor or Secondary Coolant.”

Procedural Step:

STEP	ACTION/EXPECTED RESPONSE	RESPONSE NOT OBTAINED
17	**CHECK If RCS Is Intact Inside Containment:** a. **CHECK** containment pressure - NORMAL **AND** b. **CHECK** containment radiation - NORMAL • R-2 • R-7 **AND** c. **CHECK** Containment Sump A level - NORMAL 1. Annunciator Containment Sump A Level High - CLEAR • 47031-Q 2. Annunciator Containment Sump A Level Hi-Hi - CLEAR • 47031-P **AND** d. **CHECK** Containment Sump B level- NORMAL • Channel 1 • Channel 2	**PERFORM** the following: 1. **DO NOT CONTINUE** until Attachment A complete. 2. **GO TO** E-1, LOSS OF REACTOR OR SECONDARY COOLANT.

Node 3: Successful transfer to ES 1.2 at E-1 step 22

The operators would then proceed through the steps of procedure E-1, checking if reactor coolant pumps should remain running, checking the status of RCS subcooling, and checking if any Steam Generator (SG) is faulted and maintaining intact SG levels. Additional checks are done on pressurizer PORVs and block valves and SI and Containment Isolation are then reset in E-1 Steps 6 and 7, respectively. The relevant E-1 procedure step is Step 22, which directs the operators to check if RCS cooldown and depressurization is required. It is estimated that the operators would reach and complete diagnosis of E-1 step 22 in approximately 40 minutes.

As shown below, Step 22b in procedure E-1 directs the operators to transition to procedure ES-1.2 to initiate post-LOCA cooldown and depressurization when RCS pressure is greater than 270 psig, which it will be in this case. After checking the Fold out page, operators access and follow ES-1.2.

Procedural Step:

22	**CHECK If RCS Cooldown And Depressurization Required:**	
	a. **CHECK** RCS pressure - GREATER THAN 270 PSIG [300 PSIG]	a. **IF** RHR loop flow greater than 600 gpm, **THEN GO TO** Step 23.
	b. **GO TO** ES-1.2, POST LOCA COOLDOWN AND DEPRESSURIZATION	

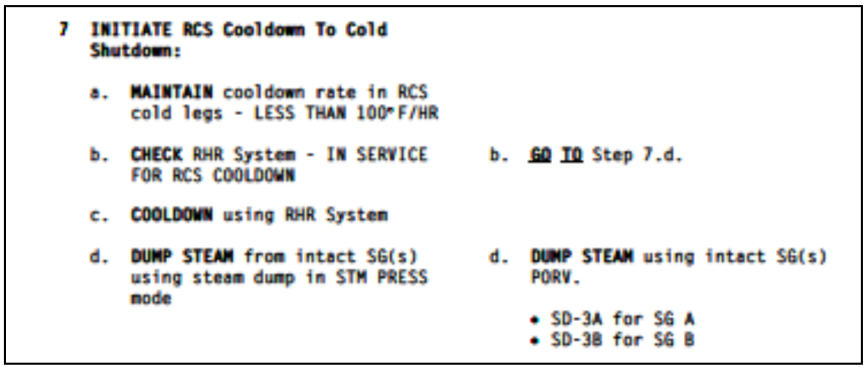
Node 4: Successful initiation and execution of cooldown at step 7 of ES 1.2

The operators will proceed through ES 1.2, and at step 7 begin cooldown and depressurization of the RCS. The performance of the cooldown and depressurization is a prolonged control action with continuous potential for mid-course corrections. This has been modeled as one node for execution, because there is no real diagnosis and there are no kick-outs once the operators enter ES-1.2 until they perform Step 7. There is a note in the procedure above Step 7 that

indicates that it needs to be done as quickly as possible without exceeding the specified cooldown rate. RWST level is still high because it is a small LOCA, so none of the fold-out page conditions are met at this point.

This can be considered as a continuous control action (i.e., an action that relies on system feedback or is a series of manipulations or control tasks) but it is straight forward to implement; execution actions are steps 7-10 of ES-1.2. In addition, there is no recovery of the execution.

Procedural Step:



7	**INITIATE RCS Cooldown To Cold Shutdown:**	
a.	**MAINTAIN** cooldown rate in RCS cold legs - LESS THAN 100°F/HR	
b.	**CHECK** RHR System - IN SERVICE FOR RCS COOLDOWN	b. **GO TO** Step 7.d.
c.	**COOLDOWN** using RHR System	
d.	**DUMP STEAM** from intact SG(s) using steam dump in STM PRESS mode	d. **DUMP STEAM** using intact SG(s) PORV. • SD-3A for SG A • SD-3B for SG B

Node 5: *Recovery – Return to step 10 from step 30 of E-0*

If the operators did not transfer to E-1 at step 17 of E-0, but continue to work through E-0, step 30 directs them back to step 10, affording another chance to get it right on Step 17.

Node 6: *Recovery – Step 23a RNO (E-1) on RWST level returns to step 16 of E-1*

If the operators proceed to Step 23 rather than transfer to ES-1.2, they are directed to return back to Step 16.

Table A.3.1 Task analysis table

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information
2	1	Check indications of RCS integrity and correctly transfer to E-1	Locate the appropriate indicator(s). Read the numerical value correctly. Understand that the indication is not in the normal range.	See node description above for specifics
3	2	Check indications if RCS cooldown and depressurization required and transfer to ES-1.2	Locate the appropriate indicator (RCS pressure). Read the numerical value correctly. Understand that the indication is above the specified pressure.	See node description for specifics
4	3	Cooldown and depressurize the RCS per procedural directions.	Since this is modeled as a complex action, there is no need to document the various activities, which include manipulation of equipment and monitoring of trends of pressure and temperature. The CFM for failure to execute a complex procedure does not distinguish between the various activities.	Prolonged control action.

A.3.3 Timeline

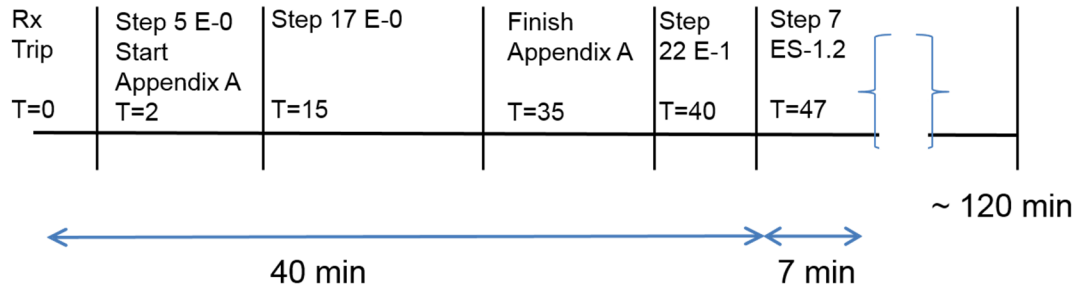


Figure A.3.3 Timeline

The timeline was constructed after consultation with operations staff. In this scenario the CVCS cannot maintain Reactor Coolant System (RCS) inventory control, and an automatic Reactor Trip occurs on pressurizer low pressure (T=0). The operators will immediately enter E-0, perform the immediate actions (steps 1-4) and reach step 5 in approximately 2 minutes, where they will start Appendix A. Operators should reach step 17 in E-0 about 13 minutes later. They will have to finish Appendix A before proceeding, which will occur about 35 minutes into the scenario. Operators will then transition to E-1, and it will take about 5 more minutes (T=40) for

them to reach step 22, and transition to ES-1.2. The operators should reach step 7 in ES-1.2 in approximately 7 minutes, at which point they will begin cooldown and depressurization.

Thermal hydraulic calculations estimate that RCS cooldown and depressurization should begin within 2 hours to avoid depletion of the RWST. This operational story and timeline are deemed feasible, given that operators should be able to start cooldown within 47 minutes of the reactor trip.

A.3.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees (DTs)

Table A.3.2 CFM selection table – Critical Task 1

CRD Node	2 – Transfer at step 17 in E-0	
Critical Task	1 – Check indications for RCS integrity	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	No	n/a. Response of this node is to a procedural step, not alarm.
AP-1: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable – Step 17 of E-0.
SA-1: Data Misleading or Not Available	No	n/a. For this PRA scenario there is no misleading data.
SA-2: Wrong Data Source Attended To	No	**Applicable in principle but screened out**. Multiple parameters in step 17, any one of which if off-normal (the case for this scenario) leads to the transition. Furthermore, since SI has initiated automatically, the off-normal readings would be expected. Therefore, the wrong source would have to be looked at for four indications, which is considered highly unlikely.
SA-3: Critical Data Misperceived	No	**Applicable in principle but screened out**. Multiple parameters in step 17, any one of which if off-normal leads to the transition. Therefore, four indications would need to be misperceived.
SA-4: Critical Data Dismissed/Discounted	No	n/a. No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	n/a. Not a monitoring task.
RP-1: Misinterpret Procedures	No	n/a. Applicable in principle, but it is judged that the procedure is clear enough that it is not open to misinterpretation.
RP-2: Choose Inappropriate Strategy	No	n/a. No viable alternative.
E-1: Delay Implementation	No	n/a. Not an execution step.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	n/a. Not a monitoring task.
E-3: Fail to Initiate Execution	No	n/a. Not an execution step.
E-4: Fail to Correctly Execute Response (Simple Task)	No	n/a. Not an execution step.
E-5: Fail to Correctly Execute Response (Complex Task)	No	n/a. Not an execution step.

Table A.3.3 Assessment of CFM applicable to Critical Task 1

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	Assessment	Justification
Workload	LOW	Crew is focused on E-0 at this point without other distractions
Procedure	SIMPLE	E-0 is very well trained on and understood. Step 17 is clear and simple.
Compensatory Factors	N/A	This branch is not applicable when the procedures are simple and workload is low.
Recovery Potential	YES	Time permits looping back through procedure to catch step again. There is a cue in E-0 Step 30 to loop back to step 10, which will lead them to step 17 again.
Crew Failure Scenario #		14

Table A.3.4 CFM selection table – Critical Task 2

CRD Node	3 - Transfer to ES 1.2 at E-1 step 22	
Critical Task	2 – Check indications if RCS cooldown and depressurization required	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	No	n/a. Response of this node is to a procedural step, not alarm.
AP-1: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable – key procedural step is Step 22b of E-1.
SA-1: Data Misleading or Not Available	No	n/a. No misleading data.
SA-2: Wrong Data Source Attended To	No	n/a. Only one parameter; can't be confused with other source.
SA-3: Critical Data Misperceived	Yes	Applicable – Parameter to be checked is high pressure but good HSI, low workload, and opportunity for recovery.
SA-4: Critical Data Dismissed/Discounted	No	n/a. No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	n/a. Not a monitoring task.
RP-1: Misinterpret Procedures	No	n/a. Applicable in principle, but it is judged that the procedure is clear enough that it is not open to misinterpretation.
RP-2: Choose Inappropriate Strategy	No	n/a. No viable alternative.
E-1: Delay Implementation	No	n/a. This is a standard well-trained small LOCA scenario. There is no viable alternative or reason to delay entry to ES-1.2.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	n/a. Not a monitoring task.
E-3: Fail to Initiate Execution	No	n/a. Not an execution step.
E-4: Fail to Correctly Execute Response (Simple Task)	No	n/a. Not an execution step.
E-5: Fail to Correctly Execute Response (Complex Task)	No	n/a. Not an execution step.

Table A.3.5 Assessment of CFMs applicable to Critical Task 2

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	Assessment	Justification
Workload	LOW	Crew is focused on controlling maintaining RCS level with SI; no other functions are challenged at this point.
Procedure	SIMPLE	Step 22b is a simple process and the crew is very familiar with E-1.
Compensatory Factors	N/A	This branch is not applicable when the procedures are simple and workload is low.
Recovery Potential	YES	If step 22 is skipped or the data misperceived, Step 23a of ES-1.2 asks if the RWST level is less than 37%, which will not be the case at this point, and the RNO loops the operators back to step 16 of E-1 and provides a recovery if the transfer step is missed initially.
Crew Failure Scenario #		14

SA-3: Critical Data Misperceived		
PIF	Assessment	Justification
HSI/Environment	GOOD	Parameter is an important one, therefore HSI is presumed not to be poor.
Workload	LOW	Scenario is a nominal SLOCA for which the procedural direction is clear, therefore workload is not considered to be high.
Training	GOOD	Training on a LOCA scenario with commonly used EOPs is expected to be good.
Recovery Potential	YES	If step 22 is skipped or the data misperceived, Step 23a of ES-1.2 asks if the RWST level is less than 37%, which will not be the case at this point, and the RNO loops the operators back to step 16 of E-1 and provides a recovery if the transfer step is missed initially.
Crew Failure Scenario #		16

Table A.3.6 CFM selection table – Critical Task 3

CRD Node	4 - Initiation and execution of cooldown at step 7 of ES 1.2	
Critical Task	2 – Cooldown and depressurize RCS	
CFMs	Applicable? (Yes/No)	Justification
AR: Key Alarm not Attended to	No	n/a. Response of this node is to a procedural step, not alarm.
AP-1: Misread or Skip Critical Step(s) in Procedure	No	n/a. Procedure unambiguous.
SA-1: Data Misleading or Not Available	No	n/a. No misleading data.
SA-2: Wrong Data Source Attended To	No	n/a. Only one parameter; can't be confused with other source.
SA-3: Critical Data Misperceived	No	n/a. Clear presentation of information with no real diagnosis.
SA-4: Critical Data Dismissed/Discounted	No	n/a. No viable alternative.
SA-5: Premature Termination of Critical Data Collection	No	n/a. Not a monitoring task.
RP-1: Misinterpret Procedures	No	n/a. Procedure unambiguous.
RP-2: Choose Inappropriate Strategy	No	n/a. No viable alternative.
E-1: Delay Implementation	No	n/a. Procedural direction to implement as fast as possible and no other viable alternative.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	n/a. Not a monitoring task.
E-3: Fail to Initiate Execution	Yes	Applicable – procedural direction is to initiate depress & cooldown.
E-4: Fail to Correctly Execute Response (Simple Task)	No	n/a. This is not a simple execution.
E-5: Fail to Correctly Execute Response (Complex Task)	Yes	Applicable – "complex" is used as surrogate for control action.

Table A.3.7 Assessment of CFMs applicable to Critical Task 3

E-3: Fail to Initiate Execution		
PIF	Assessment	Justification
Immediacy	YES	Note in the procedure above Step 7 indicates that the action needs to be performed as fast as possible.
Workload	N/A	
Recovery Potential	N/A	
Crew Failure Scenario #		8

E-5: Fail to Correctly Execute Response (Complex Task)		
PIF	Assessment	Justification
Execution Straightforward	NO	Control actions are, by definition, not straightforward.
Training	GOOD	Training on this scenario is presumed to be good.
Work Practices	GOOD	Procedure identifies hold point (<100F/hr) and check point (RHR system); standard work practice for operators to verify actions.
Recovery Potential	NO	Recovery potential n/a for control actions.
Crew Failure Scenario #		7

A.3.5 Summary of Analysis

This scenario is a routinely practiced SLOCA scenario with no complications or distractions from other equipment failure. Therefore the crew complement is assumed to be nominal as are all conditions. The procedural path is clear and the time window allows for some recovery if the crew deviated from this path, which in itself is unlikely given the clarity of the procedures and the training received. The reactor has scrammed and the crew enters E-0 and verifies that SI has initiated as required. AFW automatically initiates to remove decay heat, so the only critical safety function to be addressed is RPV integrity. At Step 17 in E-0 the operators transfer to E-1 and reach the step 22 to transfer to ES 1-2 to begin the cooldown and depressurization.

Appendix B. Lessons Learned from Existing HRA Methods and Activities and a Detailed Description of the Approach used for IDHEAS

B.1 Lessons Learned from Existing HRA Methods and Activities

To achieve the objective of reducing HRA variability, we first needed to understand the sources of the variability and the strengths and weaknesses of existing HRA methods with respect to variability. Such an understanding came from several documents and activities described next.

B.1.1 HRA Good Practices

The NRC established and documented Good Practices for performing and for reviewing HRAs (NUREG-1792 [1]). It provides a reference guide to the processes, individual analytical tasks, and judgments that would be expected to take place in an HRA (considering current knowledge and state-of-the-art) in order for the HRA results to sufficiently represent the anticipated operator performance as a basis for risk-informed decisions. The document focuses on the process of performing an HRA and does not address issues related to specific HRA methods and associated theoretical frameworks, quantification approaches and data employed by the methods.

Following the introduction of the Good Practices in NUREG-1792, an evaluation of various HRA methods that are commonly used in regulatory applications was performed, with a particular focus on their capabilities to satisfy the good practices, as well as their respective strengths and limitations regarding their underlying knowledge and data bases [2].

The results of this investigation and NUREG-1792 provided a basis for addressing the SRM on HRA model differences by identifying the features needed in a HRA method and limitations for improvement. Below is a summary of some key strengths and limitations

B.1.1.1 Strengths in Current Methods

- The automation and consistent nature of software tools like the EPRI HRA Calculator [3] is a positive enhancement in HRA. It takes away some of the burden of executing the analyses and may reduce inconsistency (computer screens remind the analyst what to consider each time). Additionally, such computerization can significantly assist HRA documentation, making it easier to review and reproduce.
- The more current HRA methods examine causes that could affect not only the implementation portion of an HFE, but also the diagnostic portion. This allows for a better understanding and more thoughtfully-based qualitative insights as to potential diagnostic vulnerabilities and their effects on the HEP than if a simple TRC (time reliability correlation) model (such as those used in THERP [4] or ASEP [5], for instance), by itself, is used for diagnosis errors.
- The use of task analysis techniques (e.g., as suggested by THERP) can greatly assist in identifying and modeling HFEs and, in particular, can help to understand potential dependencies among human actions.
- Most methods explicitly address estimating human error probabilities (HEPs) and tend to provide very limited or only partial guidance for identifying and modeling human failure events (HFEs) (particularly as to how to model the human event in the PRA). Nonetheless, SHARP1 [6] and the NRC's Good Practices (NUREG-1792 [23]) cover the identification and modeling of HFEs and collectively address these aspects of the HRA process quite well. There is additional detail available in ATHEANA [7, 8] that may also be helpful.

B.1.1.2 Limitations in HRA Process

- All the methods promote, albeit at varying degrees, the preference to use a multi-disciplinary team for performing HRA, so that no potentially important performance influencing factor (PIF) is missed and a clear understanding of the performance conditions can be obtained. Further, HRA and human factors knowledge and expertise is found to be strongly desirable in the implementation of many methods. This is a desirable characteristic that is lacking in several methods. HRA methods should emphasize this preference much more strongly in their current guidance (especially those that can be very easily implemented without such expertise or corresponding training).
- Most methods address the subject of using walkdowns, talk-throughs, and simulations as part of the HRA process, yet this is not adequately or explicitly emphasized in many methods. Without such techniques to ensure the proper inputs and necessary understanding to properly judge the influencing factors and crew behavior, too much speculation or unsubstantiated judgments may be required by the HRA analyst, leading to undesirable variability in HRA results. Use of such techniques is emphasized in the good practices [1] and covered in the PRA standards [9] endorsed by RG 1.200.
- Virtually all methods agree on the framework of treating an HFE as having both a diagnostic (more cognitive) component and a response execution (implementation) component. This is a convenient logical distinction used by the various methods and is consistent with current models in the human behavior sciences. However, there is variability as to what human PIFs are explicitly treated by the methods to address errors in both the diagnostic and execution phases of human actions, and some methods allow the diagnosis phase to be ignored when crews are following a procedure after an initiating event has been diagnosed, which can lead to inadequate assessment of crew activity and influencing factors.
- Generally, and at a high level, the HRA methods that address quantification use one of three quantification approaches. One approach adjusts basic HEPs or otherwise determines the HEPs according to a list of influencing factors specifically addressed by the method. Another uses a more flexible context-defined set of factors and more expert judgment to estimate the final HEP. A third approach uses (to the extent practicable) empirical information based on simulations of accident scenarios in power plant simulators. All of these approaches have associated strengths and limitations that should be understood, so that thoughtful application of a method can be performed.
    - Empirically based quantification can provide a level of credibility in the results that may be considered superior to analytical techniques. However, as a limitation, it is not practicable to obtain empirical evidence about every human action and related conditions that may be of interest for all types of sequences. This necessitates using limited empirical evidence for situations/sequences that were not simulated, potentially questioning the suitability of applying the information to these other situations; hence, the need for thoughtful use of the limited data and appropriate justification of its applicability wherever used.
    - Similarly, methods using specific influencing factors, associated guidance, and set multipliers as measures of the effects of influencing factors, may (at least in principle) better support the ability to reproduce results, compare results for different human actions, and lessen unwanted variability when implementing the method. However, because of the generally fixed approach of such methods, the ability to evaluate or even identify, for instance, other potentially relevant influencing factors not covered by the method, or account for interactions among the influencing factors, can be difficult and require modified use of the method or other compensations with little guidance.
    - Methods that more generally tend to employ a process whereby the analyst is freer to investigate the overall context associated with a human action and decide, through a

systematic process, what influencing factors to address and how to weigh their effects, provide a level of flexibility desirable to ensure the most relevant factors and even interactions among the factors are indeed addressed. However, without prescribed or otherwise calibrated quantification guidance to fit the myriad combinations of factors that may come up, such flexibility may lead to greater analyst to analyst variability in results.

In conclusion, it should be noted that all methods use models and other knowledge and data as the underlying bases for how they approximate the realities of human performance. In addition, all use assumptions and other judgments that, given the current state of the art in HRA, still need to be supported with appropriate data. Some bases for some methods are weaker than others and, with the continued advances and expected evolution in HRA methodology, it is expected that some methods will become less used while others, or even new methods, become more prevalent. This does not suggest that current methods cannot be used successfully in the sense that for many applications, reasonable estimates of HEPs can be obtained and potential problem areas can be identified. In fact, for the risk-informed decisions that need to be made, there have been successful uses of PRA and HRA for general risk-assessments of operating plants and for applications such as ranking components for the Maintenance Rule, changing technical specifications, and performing evaluations in the significance determination process (SDP), among others.

B.1.2 Lessons Learned from NUREG-1852 and NUREG-1921

The EPRI/NRC-RES Fire Human Reliability Guidelines (NUREG-1921 [10]) provides a method and associated guidance for conducting a fire HRA. The method includes guidance for performing the identification and definition of fire HFEs, the qualitative analysis to support modeling the fire context, and several approaches for quantification, including screening, scoping and detailed assessments. The detailed methods are extensions of EPRI's CBDT [11] and the NRC's ATHEANA [7, 8] methods (methods also supporting the development of IDHEAS) and strive to capture the potential effects of fire on human reliability. NUREG-1921 built on the lessons learned from previous NRC work on demonstrating the feasibility and reliability of operator manual actions in response to fire (NUREG-1852 [12]), but also extended HRA guidance for how to conduct a good qualitative analysis to capture a broad range of issues that could impact operating crew performance. In particular, guidance for important issues to be addressed in estimating the time required for operators to perform actions modeled in the PRA (a key aspect of HRA qualitative analysis) and the use of time margins to support the reliability of the actions were provided by the method. These improvements in how to perform qualitative HRA analysis, along with the lessons learned from the method reviews discussed above and the NRC sponsored empirical studies [13, 14] described in the next section, have been incorporated into the IDHEAS method and have significantly advanced the guidance for performing qualitative HRA analysis.

B.1.3 Findings from HRA Empirical Studies

The comparison of the methods against the analysis criteria and previous work on the good practices within HRA provides an understanding on useful features and limitations or gaps in current HRA methods. This knowledge was expanded upon with the lessons learned from the recent international and domestic HRA empirical studies [13, 14]. The goal of the international empirical study [13] was to "benchmark" HRA methods by comparing HRA predictions to empirical data generated through crew simulator runs and to empirically assess, on the basis of the data, the general strengths and weaknesses of a variety of HRA methods. The US empirical study [14] aimed to verify and extend the results and insights obtained from the international study, with a particular focus on the HRA methods used in the US and analysis teams from the US. Furthermore, the US study addressed analyst-to-analyst variability (method reliability)

through a study design with two to three analysis teams per HRA method. These are landmark studies that produced significant insights for the strengths and weaknesses of HRA methods and HRA practices and identified needed improvements in HRA. The major findings from these studies include the following:

- Cognitive basis. Both studies identified that all methods have limitations in modeling and quantifying human performance under various conditions. At least part of the effect can be attributed to a lack of an adequate underlying theoretical basis to guide the analysis, particularly with respect to the cognitive activities associated with understanding the more challenging situations and deciding how to respond. The empirical studies provide evidence that both inter-method and inter-analyst variability, in addition to other factors, is due to lack of an adequate technical basis. The assumptions made about how people can fail and why, when applying a specific method are made on the basis of analysts' understanding of plant and human behavior. HRA methods provide a technical basis for determining human performance issues and developing assumptions about how and why crews may not accomplish a safety action. The why is typically expressed in terms of performance shaping factors (PSFs), which ultimately are used in the estimation of HEPs. The empirical studies show that deficiencies in the theoretical models impact analyst capability to appropriately characterize the tasks analyzed and the associated PSFs, limit the development of a good operational understanding, and can have a large effect on the HEP. For example, inadequate evaluation of crew diagnostic tasks (cognitive activities) while they are following procedures appears to have led to optimistic HEPs, resulted in less sensitivity to important factors, and led to a lack of discrimination among HFEs in terms of their degree of difficulty. The main implication of this finding was that HRA methods need to treat carefully the cognitive aspects of human performance in working through emergency operating procedures (EOPs) and related procedures, diagnosing the situation, and deciding what to do, even if they have entered the correct procedures and understand what the basic problem or event is.
- Qualitative analysis. Systematic and thorough guidance for performing a qualitative assessment to support HRA quantification appears to be inadequate for most (if not all) methods. The differences in the qualitative analysis required by the different methods (and those performed by different analysts) appears to be a major driver of the variability and inaccuracy in the results obtained by the different applications. Improved guidance for performing the qualitative analysis should contribute to improving both the consistency and validity of HRA results.
- Tie between qualitative analysis and quantification. Many newer methods focus on identifying failure mechanisms, including the contextual factors that drive or cause them (ATHEANA [7, 8], CESA [15], MERMOS [16], CBDT [11]) and these methods generally produced a superior qualitative analysis (richer in content and better operational stories). However, superior qualitative analysis itself does not necessarily produce more reasonable HEPs. Therefore, a good tie between the qualitative analysis and the quantitative analysis is needed. Most methods have inadequate guidance on how to use the information from qualitative analysis to determine HEPs (i.e., translating the information into the inputs to the quantification of HEPs). That is, even when analysts went beyond the guidance provided by a given method for performing the qualitative analysis, it was often difficult to use the information effectively and consistently.
- PSF coverage. Most methods do not seem to cover an adequate range of PSFs or causal factors in attempting to predict operating crew performance for all circumstances. That is, important aspects of accident scenarios were not always captured by the factors considered by given methods.

- PSF judgments. Looking across methods (similar and different), there are inconsistent judgments about which PSFs (e.g., high vs. low workload, adequacy of indications) are important and how strongly PSFs affect HEPs in a given situation. The methods do not provide adequate guidance for these judgments.
- Crew variability. Crew characteristics such as team dynamics, work processes, communication strategies, sense of urgency, and willingness to take knowledge-based actions were observed to have significant effects on individual crew performance. In addition, different crews adopted different operational strategies or modes to address the scenario conditions and this was seen to have the potential to result in different scenario evolutions given the same initiating event. However, dealing with crew variability in HRA is a difficult issue. The objective of PRA and HRA is generally to model/assess average performance and many methods (e.g., SPAR-H [17], ASEP [5], CBDT [11], HEART [18]) are designed to evaluate "average" crew performance. While detailed context methods like ATHEANA [7, 8] and MERMOS [16] can in principle address crew variability, it is difficult to observe enough crews in enough situations to be able to make reasonable inferences about systematic effects for a prospective analysis for use in a PRA. How to address crew variability remains an outstanding issue in HRA.

Since the limitations of the various methods and HRA in general were identified through these mentioned efforts it became apparent that the SRM project should focus on improving HRA as a whole. It should build on the lessons learned from the empirical studies, capitalizing to the extent possible on what appeared to be useful conceptual and methodological features of the different methods and HRA processes. Since no existing single method adequately addressed inter-analyst variability, the needed range of conditions, and the other identified limitations, the SRM option of developing a new method that could be generalized with minimal adaptation to address the range of HRA domains and conditions relevant to NPP applications and which would be useable by both the NRC and industry (based as noted above on useful conceptual and methodological features of the different methods and HRA processes) was pursued.

B.2 Approach

We summarized the main lessons learned as the following:

1. Each existing method evaluated has its own strengths;
2. The methods do not have an explicit cognitive basis on why and how humans fail to perform tasks;
3. The methods either lack adequate guidance for qualitative analysis or lack an adequate interface for using qualitative analysis results for quantification of human error probabilities (HEPs);
4. The methods lack adequate guidance for how to assess and use PIFs.

Therefore, our approach to IDHEAS is to capitalize on the advantages of 1 and improve on 2, 3, and 4.

B.2.1 Integration of the Strengths of Existing Methods

Many strengths in existing HRA methods or practices have been explicitly or implicitly integrated into IDHEAS. Here we only describe a few examples.

Based on the lessons learned and our analysis, ATHEANA [7, 8] was thought to have the strongest qualitative analysis and provided a fairly comprehensive coverage of all the elements included within the content validity requirement. For instance, ATHEANA provides guidance for developing a full description of the context (including crew effects, plant conditions, and other influencing factors), accounts for cognitive and diagnosis failures, and strives to identify error-forcing conditions and failure paths that could contribute to HFEs. Furthermore, ATHEANA

accounts for errors of commission as well as errors of omission. However, ATHEANA does not provide a readily traceable mathematical account of the quantification of the HEPs, and it lacks standardization in the manner in which it is applied, and therefore, is subject to producing inconsistent results. Furthermore, application of ATHEANA can be time and resource intensive.

CBDT [11], on the other hand, is a causal structured approach providing a standard format that allows for traceability of the calculation of the HEP. The reliability of the method may also be fairly high, but the reliability is largely dependent on the level of the qualitative analysis done. However, the qualitative analysis conducted through CBDT lacks full coverage of all the elements specified under the content validity criterion identified as important in the empirical studies [13, 14] (particularly consideration of the appropriate range of PSFs and plant conditions). In addition, CBDT does not cover errors of commission and does not offer any guidance on how to perform task decomposition.

The HRA Good Practices (NUREG-1792 [1]) specifically provides guidance on PRA-HRA interface as well as HFE definition and identification. Further, the Fire HRA Guidelines (NUREG-1921 [10]) adapted the NUREG-1792 guidance for these areas to fire scenarios and demonstrated the applicability of the guidance. IDHEAS, therefore, adapted the NUREG-1792 guidance on PRA-HRA interface as well as HFE definition and identification.

NUREG-1852 [12] provided explicit criteria on HFE feasibility analysis and applied the criteria to fire scenarios. The Fire HRA Guidelines further provided explicit implementation guidance on applying the criteria and performing the relevant qualitative analysis. Given that the feasibility criteria in NUREG-1852 are generic (as confirmed by the authors of the document), the criteria were adapted for IDHEAS. Yet, the cognitive basis underlying IDHEAS allows for more thorough assessment of the criteria.

The HRA Good Practices [1] document provides generic guidance on assessing dependencies between the HFEs. The Fire HRA Guideline [10] complies with the guidance and provides detailed implementation guidance for treating dependencies. We analyzed the dependency treatments in existing HRA methods and concluded that the Fire HRA Guidelines [10] represent the state-of-practice. While we proposed new approaches to dependency based on the IDHEAS framework, we recommend that the guidance on dependency treatment in Fire HRA Guidelines is an off-the-shelf tool that can be used until the new approaches are fully developed and tested.

B.2.2 Psychological Literature Review

An understanding of human information processing and the associated cognitive mechanisms that could lead to human errors is important for understanding how crews might fail in performing their tasks. That is, it is important for an HRA model to have the ability to address the potential origin and cause of undesirable human performance in accident situations. This requires an understanding of the mechanisms of human performance that could lead to failure, as well as an understanding of how various contextual factors can influence the mechanisms and lead to undesirable human performance. Thus, a literature review of a broad range of cognitive models was performed to identify categories of cognitive mechanisms that could lead to human failures in the various phases of human information processing and the error-promoting contextual factors that could contribute to failures of those mechanisms. The literature review is discussed in more detail by Whaley et al. [19].

A key output of the literature review was the elaboration of a cognitive framework that establishes links between PIFs and cognitive mechanisms that ultimately lead to human performance failure. In order to make these linkages, the literature review identified proximate causes, which can be seen as categories of related psychological mechanisms that can lead to failures in cognitive functions such as information detection, situation assessment, and decision

making. In turn, it is these proximate causes that are the most immediate, inferable and predictable causes of operating crews failing to provide a critical function (e.g., cues/information not attended to or incorrect, incomplete, or inaccurate information used to understand the situation).

The proximate causes can be categorized into five overarching themes representing macrocognitive functions of:

1. Detecting/noticing
2. Sensemaking/understanding
3. Decision making
4. Action implementation
5. Team coordination

These macrocognitive functions may be represented at a higher level by the IDA model [20], which divides tasks into three main blocks: collecting information (I), making decision about what to do (D), and implementing the action (A). The more detailed framework of the macrocognitive functions and further refinement into the cognitive mechanisms is needed to effectively identify the cognitive basis underlying human failures. The results of the literature review provides the basis for the quantification model in that they identify the various cognitive mechanisms that can lead to failure and more importantly the factors that need to be modeled to assess the probability of their failure.

The use of the literature review [19] and the effort made to tie the factors that can influence human failures to how the crews could fail was one action taken to improve the qualitative analysis performed to support the HRA quantification. The literature review enabled a greater focus on the cognitive aspects of human behavior within the qualitative analysis and, therefore, also improved the quantitative analysis by improving understanding of the influence of contextual factors. This focus on the cognitive aspects of human behavior addressed one of the limitations demonstrated in the empirical studies [13, 14] in which it was shown to be an important contributor to crews' understanding and appropriate response to accident scenarios. It should be noted that the need to cover a broader range of factors such as those identified by the literature review was also a major emphasis of the ATHEANA HRA methodology [7, 8], which used a higher level psychological information processing model [21, 22] as a guide in developing the methodology. However, the literature review performed for this project was more extensive in terms of the breadth and depth of the cognitive models covered. In addition, the literature review results, such as the identified proximate causes and links between situational factors and identifiable manifestations of the way the crews will fail (i.e., crew failures modes [CFMs] which are discussed further below and in Chapter 5), provided the means to develop a structured, causal model for quantification (conceptually similar to the CBDT methodology [11]) that should improve reproducibility and consistency in results.

B.2.3 Development of IDHEAS- the Qualitative Analysis Structure and Quantification Model

B.2.3.1 The Qualitative Analysis Structure

One of the lessons learned from the international and domestic empirical studies [13, 14] as well as from a comparison of several HRA methods against analysis criteria determined to be important to an HRA method [23] indicated that the qualitative analysis done by most methods within HRA could be improved upon. The Fire HRA Guidelines (NUREG-1921 [10]), recently developed by the NRC and EPRI, echoes the need for developing a qualitative analysis of depth and substance and offers guidance for doing so. The guidance is based on issues covered in the PRA Standard [9], SHARP1 [6], ATHEANA [7, 8], NUREG-1852 [12], and NUREG-1792 [1].

The Fire HRA Guidelines [10] explain the goals of the qualitative analysis as, “The objectives of the qualitative analysis are to understand the modeled PRA context for the HFE, understand the actual ‘as-built, as-operated’ response of the operators and plant, and translate this information into factors, data, and elements used in the quantification of human error probabilities. A sound qualitative analysis allows the HRA to provide feedback to the plant on the factors contributing to the success of an operator action and those contributing to the failure of an operator action. ” The guidelines point out that the qualitative analysis plays two important roles: first it may be used in the identification and definition of HFEs, and next, it is used in the development of HEPs for HFEs. The qualitative analysis allows for the defining and understanding of the context relating to and driving the HFE, and therefore is crucial for feeding all the information into the quantification process.

An approach for performing the qualitative analysis is needed to represent and quantify HFEs in a PRA model that is supported by models from cognitive psychology. The qualitative analysis process includes the following in sufficient detail to support the quantification using the approach below:

- Guidance for determining the PRA definition for the HFE (often referred to as the PRA scenario context);
- Guidance for performing a task analysis and the identification of the possible operator failures that could lead to failure of the HFE.
- Guidance for developing Crew Response Trees (CRT) (alternatively Procedural Failure Path Trees [PFPT) to represent the potential human failure and recovery paths through the procedures that could affect the probability of the HFE.
- Guidance for identifying applicable Crew Failure Modes (CFMs) that could contribute to the likelihood of different failure paths and their recovery.
- Guidance for collecting the information necessary to understand the plant conditions and PSFs in order to correctly apply the decision trees to quantify the CFMs and ultimately the pre-defined HFEs in the PRA model.

To make the qualitative analysis transparent and traceable, we intended to develop a layered qualitative analysis structure that analyzes human failures in PRA scenarios in progressive details. The structure included the following parts:

- Scenario understanding – qualitative analysis should begin with an understanding of the PRA scenario, the operational events, system functions involved in these events and human actions required to achieve the functions.
- Event analysis – This included identifying and defining HFEs in the scenarios, and assessing the feasibility of the HFEs; only the feasible HFEs will go to the next step of analysis
- Task analysis within an event – This is to identify the tasks that operators perform in an HFE and further identify those critical tasks that failing any of them would result in the failure of the HFE. Not all the tasks are essential; some are confirmatory, and performing them incorrectly would not necessarily lead to failure. However, they may be relevant as recovery factors, and they certainly contribute to using up available time.
- Cognitive task analysis for every critical task – This is to provide information for quantifying the failure of the critical tasks and the HFE.

The outcomes of these analysts are integrated in the quantification process.

B.2.3.2 HFE Quantification

One of the findings from the empirical studies [13, 14] was that methods that focus on identifying failure mechanisms and the contextual factors that drive or cause them (e.g.,

ATHEANA [7, 8], CESA [15], MERMOS [16], CBDT [11]), generally produced a superior qualitative analysis (richer in content and better operational stories) than other methods. However, they did not always produce HEPs that reflected the empirical results. It was recognized that a broad range of PIFs and careful consideration of crew cognitive activities are needed to appropriately quantify HFEs. As discussed earlier, the cognitive basis we developed through the literature review [19] is used to address these issues by helping to identify the set of causal factors associated with various cognitive mechanisms that can lead to failure and determine what factors need to be modeled for a given scenario.

CBDT [11] is based on a causal model approach and the decision trees (DTs) used to quantify the different crew failure modes (CFMs) lend themselves directly to using the results from the literature review (and the CBDT approach with wide industry usage has been shown to be a useful, if not perfect quantification tool). Thus, we selected the use of DTs as a structured approach for quantifying HFEs. This approach requires having the details of the following elements:

- A set of Crew Failure Modes (CFMs) that adequately and specifically describes the various kinds of failures of the critical tasks in NPP events;
- A set of Decision Trees (DTs), one for each CFM, to illustrate possible paths to the CFMs;
- The PIFs addressed in those trees to determine the probability of the human failure scenarios that could lead to the CFMs, based on a detailed review of the psychological literature to identify the cognitive mechanisms that could lead to the CFMs and the associated PIFs that could contribute to the occurrence of the cognitive mechanisms;
- A set of questions for each DT branch to determine the DT paths;
- A set of HEPs estimated through expert judgment and assigned to each CFM and DT path.

Just as the psychological literature review drew inspiration from the IDA model [20] in directing the search for cognitive mechanisms of interest, the CFMs also reflect this categorization scheme. Fourteen CFMs were identified and map to three stages of the crew interaction with the plant. The three stages resemble the IDA model and are: status assessment, response planning, and action/execution. These stages are proposed to occur sequentially; that is, progressing to a later stage assumes success in the previous stage(s). A majority of the CFMs identified fall within the status assessment phase. These CFMs are ways of failing the tasks related to obtaining and processing the critical data required to make a correct plant status assessment (e.g., key alarm not attended to, critical data not obtained, critical data dismissed/discounted). CFMs within the response planning stage assume a correct plant status assessment has been done, but an error occurs in formulating the response and deciding upon a course of action. Finally, CFMs within the final stage of action cover errors that occur in either performing the action incorrectly (i.e., an error of commission) or in not performing the action at all (i.e., an error of omission). Each of the CFMs is represented in a DT, and the branch points of the DTs correspond to the PIFs considered to be most relevant to the cognitive mechanisms that can result in the CFM.

The quantification model, which addresses the set of relevant CFMs and different paths through the CRT for a given HFE, has the following form for a given scenario, S, with an associated context:

$$HEP(HFE|S) = \sum_{CRT\ sequence} \sum_{CFM} Prob(CFM|CRT\ sequence, S)$$

where the outer sum is over the CRT sequences that leads to the HFE, and the inner sum is over the CFMs that are relevant for the CRT sequence. The term $Prob(CFM|CRT\ sequence, S)$ is the probability associated with the end point of the path through the DT for the specific CFM that

is determined by the assessment of the relevant contextual factors associated with the HFE (and the CRT sequence). These contextual factors will be determined by answering the questions associated with the DT branches; the point of each path will be provided with an HEP that will be obtained through an expert judgment elicitation and included in the DTs for the users of the method.

Taken together, the assets of the method provide a means to perform a broad and thorough qualitative analysis that will capture the important aspects of the accident scenario conditions and PSFs likely to influence operating crews, including potential crew failure paths, and provide a structured and systematic approach for reliably quantifying HFEs in the context of a PRA. In addition, the basic approach will ultimately be generalizable to other PRA domains (with some domain specific adjustments) beyond full-power operation, to which the current method is tailored.

B.3 References

1. 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.
2. Forester, J., Kolaczkowski, A., Lois, E., & Kelly, D. (2006). Evaluation of Human Reliability Analysis Methods against Good Practices. (NUREG-1842). Washington, DC: US Nuclear Regulatory Commission.
3. Julius, J., Grobbelaar, J., Spiegel, D., & Rahn, F. (2005). The ERPI HRA Calculator® User's Manual, Version 3.0. Palo Alto, CA: Electric Power Research Institute.
4. Swain, A. D. & Guttmann, H. E. "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications." NUREG/CR-1278/SAND80-0200, Sandia National Laboratories for the US Nuclear Regulatory Commission, Washington, DC, August 1983.
5. Swain, A. D. "Accident Sequence Evaluation Program Human Reliability Analysis Procedure." NUREG/CR-4772/SAND86-1996, Sandia National Laboratories for the US Nuclear Regulatory Commission, Washington, DC, February 1987.
6. Wakefield, D., Parry, G., Hannaman, G., & Spurgin, A. (1992). SHARP1: A Revised Systematic Human Action Reliability Procedure. (EPRI TR-101711, Tier2). Palo Alto, CA: Electric Power Research Institute.
7. Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA) (2000). (NUREG-1624, Rev. 1). Washington, DC: US Nuclear Regulatory Commission.
8. Forester, J., Kolaczkowski, A., Cooper, S., Bley, D., & Lois, E. (2007). ATHEANA User's Guide. (NUREG-1880). Washington, DC: US Nuclear Regulatory Commission.
9. 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.
10. 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.
11. Parry, G., Lydell, B. O. Y., Spurgin, A. J., Moieni, P., & Beare, A. (1992). An Approach to the Analysis of Operator Actions in PRA. (EPRI TR-100259), Palo Alto, CA: Electric Power Research Institute.
12. Kolaczkowski, A., Forester, J., Gallucci, R., Bongarra, J., & Lois, E. (2007). Demonstrating the Feasibility and Reliability of Operator Manual Actions in Response to Fire. (NUREG-1852). Washington, DC: US Nuclear Regulatory Commission.

13. Lois, E., Dang, V. N., Forester, J., Broberg, H., Massaiu, S., Hildebrandt, M., Braarud, P. Ø., Parry, G., Julius, J., Boring, R., Männistö, I., & Bye, A. (2009). International HRA Empirical Study – Phase 1 Report: Description of Overall Approach and Pilot Phase Results from Comparing HRA Methods to Simulator Data. (NUREG/IA-0216, Vol. 1). Washington, DC: US Nuclear Regulatory Commission.
14. Forester, J., Hildebrandt, M., Broberg, H., Nowell, R., Liao, H., Dang, V. N., Presley, M., Bye, A., Marble, J., Lois, E., Hallbert, B., and Morgan, T. (2011). US HRA Empirical Study -- Comparison of HRA Method Predictions to Operating Crew Performance in a US Nuclear Power Plant Simulator and an Assessment of the Consistency of HRA Method Predictions (Draft Report).
15. Reer, B., Dang, V. N., & Hirschberg, S. (2004) The CESA method and its application in a plant-specific pilot study on errors of commission. Reliability Engineering & System Safety, 83, 187-205.
16. Bieder, C., Le-Bot, P., Desmares, E., Bonnet, J-L., & Cara, F. (1998). MERMOS: EDF's new Advanced HRA Method. Proceedings of the 4th International Conference on Probabilistic Safety Assessment and Management (PSAM 4), New York, NY.
17. Gertman, D. I., Blackman, H. S., Byers, J., Haney, L., Smith, C., & Marble, J. (2005). The SPAR-H Method. (NUREG/CR-6883). Washington, DC: US Nuclear Regulatory Commission.
18. Williams, J. C. (1985). HEART – A Proposed Method for Achieving High Reliability in Process Operation by Means of Human Factors Engineering Technology. Proceedings of a Symposium on the Achievement of Reliability in Operating Plant, Safety and Reliability Society. NEC, Birmingham.
19. Whaley, A. M., Xing, J.,Boring, R. L., Hendrickson, S. M. L., Joe, J. C., LeBlanc, K. L., & Lois, E. (in preparation). Building a Psychological Foundation for Human Reliability Analysis. (NUREG-2114, INL/EXT-11-23898). Washington, D.C.: U.S. Nuclera Regulatory Commission.
20. Smidts, C., Shen, S. H., & Mosleh, A. (1997). The IDA Cognitive Model for the Analysis of Nuclear Power Plant Operator Response Under Accident Conditions. I: Problem Solving and Decision Making Model. Reliability Engineering & System Safety, 55(1), 51-71.
21. Reason, J. T. (1990). Human Error. New York, NY: Cambridge University Press.
22. Woods, D. D., Pople, H. E., and Roth, E. M. (1990). The Cognitive Environment Simulation (CES) as a Tool for Modeling Human Performance and Reliability. (NUREG/CR-5213). Pittsburgh, PA: Westinghouse Electric Corp.
23. Hendrickson, S. M. L., Forester, J. A., Dang, V. N., Mosleh, A., Lois, E., & Xing, J. (2012). HRA Method Analysis Criteria. Proceedings of the 11th International Conference on Probabilistic Safety Assessment and Management (PSAM11), Helsinki, Finland.

Appendix C. Selection of Proximate Causes (PCs), Cognitive Mechanisms, and Performance Influencing Factors (PIFs)

This appendix provides background information on the development of the quantification model (CFMs/DTs) for internal at-power events based on the Cognitive Basis Structure. The CFMs were developed to represent observable and predictable failures of a crew in response to an upset condition within a nuclear power plant (NPP). They were based on the Proximate Causes (PCs) of the macrocognitive functions. Yet, while the PCs of a given cognitive function is applicable to any human actions involving the function, the corresponding CFMs are intended to cover failures of procedural human actions performed in control-room in internal at-power events. Although the development of the CFMs was informed by the psychological literature review, the CFMs were identified from a system perspective. We developed these CFMs based on our experience and understanding of plant at-power operation in control rooms; the CFMs cover the major task types (e.g., data gathering, diagnosing, planning, manipulating, following procedures, communicating). Similarly, the PIFs were developed to represent observable and predictable features of PRA event scenarios for internal at-power events; they were based on the cognitive mechanisms identified in the Cognitive Basis Structure, yet they only represent the set of the features that are relevant to the CFM in internal at-power events. Therefore, we cannot say that the CFMs and PIFs of the DTs are complete but we believe that the current set of CFMs are good enough for internal at power events.

The appendix has two sections. The first section reviews and discusses what proximate causes (PCs), cognitive mechanisms and performance influencing factors (PIFs) were deemed to be relevant for each crew failure mode (CFM). The discussion provides the scientific basis for the CFMs and DTs. On the other hand, the second section reviews the cognitive mechanisms that were not represented through the PIFs of the DTs, with a justification that leaving those mechanisms out of the DTs was consistent with the assumptions made for this method about the HFEs for control room actions in internal at-power events.

C.1 Mapping of PCs, Cognitive Mechanisms, and PIFs for Every CFM

C.1.1 Plant Status Assessment Phase

Six CFMs are included within this phase[19]:

- AR: Key alarm not attended to
- SA-1: Data misleading or not available
- SA-2: Wrong data source attended to
- SA-3: Critical data misperceived
- SA-4: Critical data dismissed/discounted
- SA-5: Premature termination of critical data collection

During this stage of interaction between the crew and the plant, the crew is gathering information about the plant status and diagnosing or developing an understanding of the plant condition. Failures within this phase would result in an incorrect understanding of the plant status. This incorrect understanding may lead to one of two outcomes: either the crew enters the wrong procedure or, if they are already within a procedure, the crew chooses the wrong path for responding to the plant disturbance, and thereby fails the required function. Since this phase

[19] Key alarm not attended to is not pertinent to just this phase, but actually represents a special case that covers recognizing the alarm, understanding it and taking the appropriate action.

deals with developing an understanding of the plant status, the primary macrocognitive functions of interest are *Detection* and *Understanding*. *Decision-making* will be more important during the next phase of interaction; however, there are some elements early in the decision-making process that are relevant in this phase as well.

The *action execution* macrocognitive function is generally not relevant to this phase since no action is being taken. This is true for all of the CFMs except “key alarm not attended to”, which represents a special case. Because this CFM encompasses not only registering the alarm but also responding to it, it holds an element of action within it. Therefore, the PCs for the macrocognitive function of action/execution were evaluated for “key alarm not attended to”. For every other CFM within this phase, action/execution was determined to not be relevant and was not examined further.

“Data misleading or not available” also represents a special case as it really does not represent a crew failure mode, but instead is a condition that would lead the crew to fail. It is included in the list of CFMs for completeness since scenarios involving data unavailability or inaccuracy are not always included in a PRA. However, since it does not represent a true CFM, it was not evaluated with regard to the PCs and cognitive mechanisms as it is not a cognitive failure that leads to this failure state.

Finally, the team coordination macrocognitive function is covered entirely by the CFM “critical data miscommunicated”, which is a CFM that includes multiple stages of interaction. Therefore, the PCs within this macrocognitive function were not evaluated for any of the remaining CFMs. If, in the evaluation of the HFE, crew communication is thought to be a relevant factor, the CFM of “critical data miscommunicated” should be included in the analysis and it will not be addressed within the other CFMs. The PC dealing with errors in leadership or supervision is not considered for any CFM including “critical data miscommunicated” because leadership aspects cannot be evaluated at this level of HRA.

C.1.1.1 AR: Key Alarm Not Attended To

This CFM represents the failure to respond to a key alarm. For those alarms for which the response is memorized, simple, and ingrained (e.g., pressing the scram control on receipt of a scram alarm), this could also include the failure to act. This CFM is applicable to cases in which the alarm is the principal cue (and the response is typically an immediate action) or when the alarm is a trouble alarm leading to entry into an alarm response procedure. A likely cause to not attending to a key alarm is distraction or heavy workload in which the significance of the alarm is diminished by coincident alarms or other activities. Training and experience will help a crew to prioritize the response to the alarm appropriately. Additionally, the design of the alarm and the salience of it play an important role it its ability to be easily distinguishable from other controls on the panel and be understood by the crew. Table C-1 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-1. Relevant PCs, Cognitive Mechanisms, and PIFs for Key Alarm Not Attended To

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Detecting/ Noticing	Cue/information not perceived	Cue content	Workload HSI Task complexity	If distractions are high (e.g., either through a high workload such that the crew must attend to multiple responsibilities or if multiple alarms are going off) or if the design of the alarm is such that it may not be easily distinguishable from surrounding noise, the alarm may not be perceived.
	Cue/information not attended to	Cue content	HSI	Not attending to the alarm is valid under situations when there are so many alarms going off that the crew cannot differentiate between the cues. Note that some of the mechanisms and PIFs listed here may be more relevant for consideration during recovery, but not for an initial alarm.
		Vigilance in monitoring	Task load HSI (esp. in regard to trouble alarms)	
		Working memory	Task load (number of alarms) HSI	
	Cue/information misperceived	Cue content	HSI Load (work and task) Task complexity Stress Fatigue Fitness for duty	The alarm may be misperceived for a number of factors including an increased load. The increased load may refer to either a high task load in which the crew is physically tasked with multiple tasks to complete or to a high workload referring not only to the number of tasks that must be completed but also to the cognitive load of such tasks and the time pressure in which they must be done. Furthermore, additional stressors such as fatigue or a decreased fitness for duty may impact the ability of the crew to correctly perceive the alarm. Finally, the layout of the alarm panel (HSI) and/or salience of the alarm may impact its ability to be correctly perceived.
Understanding/ Sensemaking	Incorrect data used to understand the situation	N/A	N/A	This CFM assumes the correct alarm is activated, but that the crew does not attend to it. Therefore, this PC is not relevant.
	Incorrect integration of data, frames, or data with a frame	N/A	N/A	These alarms are expected to be responded to immediately and are well trained. The crew does not respond to the alarm for some other reason (e.g., distraction).
	Incorrect frame used to understand the situation	N/A	N/A	This CFM assumes that trained operators always have the ability to understand the alarm.
Decision Making	Incorrect goals or priorities	Incorrect prioritization of goals	Training Experience Task load (precondition of having multiple alarms competing for attention)	Deciding the alarm is insignificant in relation to the other stuff that is going on (in the specific HFE context).

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
			Procedures Resources (probably not for an initial alarm, but might be relevant for later in the scenario)	
	Incorrect internal pattern matching	N/A	N/A	Once an alarm sounds, the crew immediately starts on a course of action. These actions are well trained and do not rely on mental simulation or pattern matching as described in these PCs.
	Incorrect mental simulation or evaluation of options	N/A	N/A	
Action	Failed to take required action	Divided attention	Task load	The type of actions occurring for this CFM would be memorized, simple responses or retrieving the correct procedure. However, errors may occur in either not executing the action or in executing it incorrectly due to any of the cognitive mechanisms listed.
	Executed desired action incorrectly	Dual task interference	Task load HSI	
		Task switching interference	Task load HSI	
		Population stereotypes	HSI	
		Motor learning	Training	

C.1.1.2 SA-2: Wrong Data Source Attended to

This CFM describes the situation in which the crew knows they have to obtain specific information, and the desired information is available, but the crew consults the wrong source. Specifically, this CFM refers to slips in attending to the data (i.e., the crew has the right intent, but attends to the wrong target). It does *not* refer to misreading of procedures, miscommunication, misperception of the correct data, data misleading or unavailable, or having an incorrect mental model of the plant system (not the plant status per se) since these are each addressed by other CFMs. Several things may lead to this CFM such as there being more than one train available or several similar indicators are grouped together. The failures might result from slips or having an incorrect or poor mental model of the plant system (not the plant status per se but poor familiarity with the layout for example). In selecting relevant PCs and cognitive mechanisms for this CFM, many point to the development of an incorrect mental model. However, in constructing the decision tree and formulating the questions regarding the PIFs, the formation of an incorrect mental model with regards to the plant status is not relevant. Instead, it is the mental model of the plant system. The PIFs that seem most relevant are knowledge/experience and training as they pertain to the specific source, and HSI as it pertains to the ease of locating the correct source. In addition, although not explicitly identified in the mapping to cognitive mechanisms, workload is considered to be a contributor to the likelihood of making an error and is included as a PIF for this CFM. Table C.1-2 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-2. Relevant PCs, Cognitive Mechanisms, and PIFs for Wrong Data Source Attended to

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Detecting/ Noticing	All	N/A	N/A	The macrocognitive function of Detecting and Noticing refers to the process of sensing and perceiving important information in the work environment. This CFM is not referring to errors that occur during this stage of processing.
Understanding/ Sensemaking	Incorrect data used to understand the situation	Attention to wrong/inappropriate information	Cue salience HSI	This PC is directly relevant to the CFM as it based on the premise that incorrect data has been gathered and is then used to understand the situation.
		Improper data/aspects of the data selected for comparison with/identification of a frame	Knowledge/ experience/ expertise Training HSI Situation dynamics or complexity	
		Incorrect or inappropriate frame used to search for, identify, or attend to information	Knowledge/ experience/ expertise Training	
	Incorrect integration of data, frames, or data with a frame	N/A	N/A	This PC is not relevant for this particular CFM because it assumes the correct data has been gathered and the CFM is based on the premise that the data gathered is incorrect.
	Incorrect frame used to understand the situation	Incorrect or inadequate frame/mental model used to interpret/integrate information	Knowledge/ experience/ expertise Training Motivation	This PC is relevant if the frame that is incorrect is understood to be the mental model of the plant system and not the plant status. Due to an incorrect model of the plant system, the operator goes to the wrong location to gather the information.
		Incorrect or inappropriate frame used to *search for*, identify, or attend to information	Knowledge/ experience/ expertise Training	
Decision Making	All	N/A	N/A	This CFM does not deal with response planning or errors that may occur within this phase.

C.1.1.3 SA-3: Critical Data Misperceived

This CFM refers to the situation in which a critical piece of information that is required to develop a plant status assessment is misperceived. It may cover those instances in which a parameter is misread from a display or a mistake is made in determining the equipment status from indicators on the control panel. This CFM is intended to be a “local” failure at the level of the specific item of data. Therefore, in the context of this CFM, the mental model of concern is not the overall model of the plant status but rather the mental model of the source of information (i.e., it is the localized mental model) or more automatic application of mental model. The reasons why an operating crew might fail include difficulties with the source of the data, which include limits on the source’s discriminating power and its accessibility, exacerbated by a lack of

familiarity of the data source and any potential biases related to expectations on what the value of the data usually is or “always has been”. Table C.1-3 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-3. Relevant PCs, Cognitive Mechanisms, and PIFs for Critical Data Misperceived

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Detecting/ Noticing	Cue/information not perceived	N/A	N/A	For this CFM, the data are perceived and attended to, but are misperceived or misread. Therefore, these PCs are not relevant.
	Cue/information not attended to	N/A	N/A	
	Cue/information misperceived	Attention	HSI	The cue in this case refers to the data (e.g. parameter value, the parameter trend), and those data are misread. This error may occur either because, for example, the crew is distracted when reading the value, the crew lacks familiarity with how to properly read the value, or the data source is poorly designed.
		Vigilance in monitoring	Knowledge/ experience/ expertise	
			Training	
			Familiarity with the situation	
			HSI	
		Cue content	HSI	
		Expectation	Knowledge/ experience/ expertise	
			Training	
Understanding/ Sensemaking	Incorrect integration of data, frames or data with a frame	The data are not properly recognized, classified, or distinguished	HSI	The cognitive mechanisms and PIFs of this PC explain how the misperceiving might occur. This PC is not addressing the overall mental model of the plant status but rather the localized or more automatic application of the mental model.
			Knowledge/ experience/ expertise	
			Training	
			Procedure quality	
	Incorrect data used to understand the situation	N/A	N/A	The assumption for this CFM is that the data is correct but that it is incorrectly perceived; therefore, this PC, which deals with incorrect data, is not relevant.
	Incorrect frame used to understand the situation	N/A	N/A	In this case, the crew is gathering the data and is not yet to the stage of interpreting it or giving it meaning. Therefore, this PC is not relevant.
Decision Making	All	N/A	N/A	The crew is actively looking for the information and is not yet to the stage of deciding on an action.

C.1.1.4 SA-4: Critical Data Dismissed/Discounted

The crew is aware of and has obtained the correct information, but has discounted it from the assessment of the plant status. The information being dismissed is an essential part of assessing the plant status for which there is at least one successful response. This CFM represents a deliberate discounting as opposed to postponing its consideration or not obtaining the data because of misinterpreting or skipping a step in the procedure. Since the cognitive process of establishing a mental model is likely to be iterative and cyclic in nature, this CFM is applicable when an assessment of plant status that is made on partial information leads to a failure. Generally a crew or operator may dismiss or discount critical data because of a bias in

their training or knowledge/experience/expertise such that they develop an inaccurate plant status assessment. In addition, poor procedural quality or poor HSI output could exacerbate the incorrect assessment. Table C.1-4 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-4. Relevant PCs, Cognitive Mechanisms, and PIFs for Critical Data Dismissed/Discounted

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Detecting/ Noticing	All	N/A	N/A	This CFM assumes the crew is aware of and has even obtained the correct information; therefore, the macrocognitive process of Detecting/Noticing is not relevant.
Understanding/ Sensemaking	Incorrect data used to understand the situation	N/A	N/A	This PC is not relevant because the correct data was collected, but the crew decided to dismiss it.
	Incorrect integration of data, frames, or data with a frame	Improper integration of information or frames	Knowledge/ experience/ expertise	For this PC, the mental model is being formed and the piece of information does not match the projection of the mental model.
		Improper aspects of the frame selected for comparison with the data	Knowledge/ experience/ expertise	
		Incorrect or failure to match data/information to a frame/mental model	Knowledge/ experience/ expertise HSI output	
	Incorrect frame used to understand the situation	Incorrect or inadequate frame/mental model used to interpret/integrate information	Knowledge/ experience/ expertise Training Motivation	This PC is based on the idea that the crew has the wrong mental model. Having a wrong mental model may be a driving cause behind the crew dismissing the critical data.
		Frame/mental model inappropriately preserved/ confirmed when it should be rejected/reframed	Knowledge/ experience/ expertise Trust in the data source	
Decision Making	Incorrect goals or priorities set	N/A	N/A	The decision making process has not been fully entered yet so response planning is not an issue. Therefore, response options are not being considered and goals and priorities that must be achieved through the responses are not relevant to this CFM.
	Incorrect internal pattern matching	Not updating the mental model to reflect the changing state of the system	Knowledge/ experience/ expertise Training Procedures	The formation of a mental model is an iterative and cyclical process. The information that is collected is integrated into the mental model and may be used to modify it as appropriate. The error described in the CFM occurs when data necessary for informing the mental model is dismissed.
		Cognitive biases	Knowledge/ experience/ expertise Training	

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
	Incorrect mental simulation or evaluation of options	N/A	N/A	The decision making process has not been fully entered yet so response planning is not an issue. Therefore, the mental simulation of how the response options may play out is not relevant to this CFM.

C.1.1.5 SA-5: Premature Termination of Critical Data Collection

This CFM describes the situation in which the crew stops collecting data too early and then assesses the plant status on an incomplete data set. Since the data being collected is relevant to the plant status assessment, this CFM is related to the development of the mental model of the plant status. A crew may stop collecting data that would be needed to establish the true picture because an existing, incorrect mental model is supported with the existing collection. Additionally, this CFM would also apply to the case when additional, e.g., confirmatory data, should be obtained but is not and thus the wrong mental model is formed. A defining characteristic of this CFM is that the crew is able to develop a plant assessment that is viable and consistent with the partial plant status signature obtained to date. Not only does the plant status represented by the partial information have to be viable, it also has to be credible to the operators. Training, experience and knowledge play important roles in this CFM as they may either bias the operator in the direction of believing the incorrect plant status or, conversely, may help the crew overcome a bias to continue collecting data so that the correct plant status is obtained. Table C.1-5 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-5. Relevant PCs, Cognitive Mechanisms, and PIFs for Premature Termination of Critical Data Collection

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Detecting/ Noticing	All	N/A	N/A	Detection is irrelevant because the crew is able to obtain the data, but they *choose* to stop obtaining it.
Understanding/ Sensemaking	Incorrect data used to understand the situation	Incorrect or inappropriate frame used to search for, identify, or attend to information	Knowledge/ experience/ expertise Training	For this CFM, the focus is on the "incomplete" emphasis within the PC. The crew has access to the information but decides to stop collecting it based on the partial "understanding" of the plant status. This misunderstanding is the rationale for prematurely terminating data collection. Another misunderstanding may include thinking there is less time available than actually is. This CFM refers to collecting information to determine a trend and the crew might prematurely terminate data collection because they feel that they have a correct picture of the trend.
		Improper data/aspects of the data selected for comparison with/identification of a frame	Knowledge/ experience/ expertise Training HSI Situation dynamics or complexity	
	Incorrect integration of data, frames, or data with a frame	Improper integration of information or frames	Knowledge/ experience/ expertise Training	Within this context, the operator is presented with the correct data and his/her frame or mental model is correct; however, the integration of data, matching of data to frame, or updating process (for updating the frame with the data) goes awry. Specific for this CFM, a mismatch with expectations may lead the crew to an inappropriate monitoring strategy. Alternatively, the cognitive capacity of the crew or operator may be over-taxed such that only a limited amount of the situation is processed. A final alternative is the crew may be distracted away from checking the information with the appropriate frequency.
		Incorrect or failure to match data/information to a frame/mental model	HSI Knowledge/ experience/ expertise	
		Working memory limitations impair processing of information (only relevant if procedures are bad)	Procedure quality	
		Mental manipulation of the information is inadequate, inaccurate, or otherwise inappropriate	Knowledge/ experience/ expertise Training	
	Incorrect frame used to understand the situation	Incorrect or inadequate frame/mental model used to interpret/integrate information	HSI Knowledge/ experience/ expertise Training	The crew has access to the information but has developed the wrong mental model of the plant status. This wrong mental model may cause the critical data to be dismissed because the data may not fit into the (wrong) mental model.
		Frame/mental model inappropriately preserved/ confirmed when it should be rejected/reframed	Knowledge/ experience/ expertise Training Trust in the data source	
Decision Making	All	N/A	N/A	Decision is not applicable because the crew is simply making a plant status assessment, not making a response.

C.1.2 Response Planning Phase

Two CFMs are included within this phase:

- RP-1: Misinterpret procedure
- RP-2: Choose inappropriate strategy

Failures during this stage of interaction result in the crew or operator adopting an incorrect approach even though they have the correct assessment of the plant status. Because of the way the plant status CFMs have been defined, it is assumed that the crew has understood what function(s) they are supposed to be dealing with and have made a correct assessment of the plant condition. Also, since they are using procedures, the correct diagnosis means that they have transitioned into using the correct procedure.

The macrocognitive functions most relevant for this phase of interaction are Understanding/Sensemaking and Decision Making. Given success in the prior phase (i.e., plant status), it is assumed that the cognitive functions covered with Detecting/Noticing would be successful; that is, the correct information would be perceived and attended to. Therefore, the PCs for Detecting/Noticing are not evaluating any further for the CFMs within this phase. Similarly, the PCs within the macrocognitive function Action/Execution are not considered relevant for the CFMs within this Response Planning phase since no action is being taken.

Finally, as described in the previous phase ('plant status'), the team coordination macrocognitive function is covered entirely by the CFM "critical data miscommunicated". Therefore, the PCs within this macrocognitive function were not evaluated for any of the remaining CFMs. The CFM "critical data miscommunicated" is covered in Section E.4.

C.1.2.1 RP-1: Misinterpret Procedure

This CFM describes the situation in which a procedure is misinterpreted in such a way that an incorrect path through the procedures is followed or an incorrect response is initiated. Misinterpretation is most likely to occur when the procedure is written ambiguously or its structure includes complicated logic. Therefore, this CFM focuses on problems originating with the nature of the procedures. Table C.1-6 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-6. Relevant PCs, Cognitive Mechanisms, and PIFs for Misinterpret Procedure

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Understanding/ Sensemaking	Incorrect data used to understand the situation	Information available in the environment is not complete, correct, accurate, or otherwise sufficient to create understanding of the situation	Procedure availability and quality	This PC is relevant if the incorrect data referred to are the procedures being used. The procedures may be poorly written or be very complex causing the crew to misinterpret them.
		Data not properly recognized, classified, or distinguished	Procedure quality Knowledge/ experience/ expertise Training	
	Incorrect integration of data, frames or data with a frame	N/A	N/A	This PC is not relevant as it refers to the correct data being poorly integrated with the correct mental model. In the case of this CFM, the integration of the data with the model is not the issue; more likely the issue is the procedure quality.
	Incorrect frame used to understand the situation	N/A	N/A	Although problems in misinterpreting the procedures may lead to an inaccurate mental model, the inaccurate mental model is not the focus of this CFM.
Decision Making	Incorrect goals or priorities set	N/A	N/A	This PC is most relevant for novel situations in which procedures are not available. Therefore, it is not relevant for this CFM.
	Incorrect internal pattern matching	N/A	N/A	This PC is relevant when the operator or crew has mapped the situation to an inappropriate mental model. Although this CFM may lead to an inaccurate mental model, the inaccurate mental model is not the focus of this CFM.
	Incorrect mental simulation or evaluation of options	Misinterpretation of procedures	Time load Training Procedures	The procedures may be poorly written or be very complex causing the crew to misinterpret them. In addition, time may be compromised if the crew has to spend much time trying to decipher the procedure or determine which procedure is the appropriate one.

C.1.2.2 RP-2: Choose Inappropriate Strategy

For this CFM, the crew has entered the correct procedure and is presented with more than one alternative for how to proceed. This CFM also covers cases where there is judgment left to the operator (e.g., external events, implementation of SAMGs). From the choices presented to the crew, they choose the wrong alternative, leading to the HFE. This CFM assumes that the crew has the correct mental model for the scenario up until this point (i.e., knows what function(s) needs/need to be restored). Table C.1-7 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-7. Relevant PCs, Cognitive Mechanisms, and PIFs for Choose Inappropriate Strategy

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Understanding/ Sensemaking	All	N/A	N/A	This CFM assumes that the correct data is presented and the crew has formed the correct plant status assessment. The error occurs in the decision making process when the crew decides upon an incorrect course of action. Therefore, this PC is not relevant.
Decision Making	Incorrect goals or priorities set	Goal conflict	Procedures Experience Training System responses Awareness of economic consequences (perceived decision impact on plant)	This PC is relevant not because it calls into question the goal of restoring the function but because there is the trade-off in weighing the benefit of the strategy versus any downside it might have for restoring the plant. Thus, an improper weighting of the cost/benefits may lead the crew to choose a strategy or response that is less than optimal. Factors such as lack of experience, infrequent training, insufficient time and poorly written procedures are likely to play a role.
		Incorrect goal selected	Experience Training Time load	
		Incorrect prioritization of goals	Experience Training Resources Procedures	
	Incorrect mental simulation or evaluation of options	Inaccurate portrayal of the system response to the proposed action	Experience Training Procedures Available and perceived time	This CFM may be due to the crew incorrectly predicting how the system will respond to the proposed action. The cognitive bias of overconfidence may also be to blame in causing this CFM. 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.
		Cognitive bias (overconfidence)	Experience Training	

C.1.3 Action/Execution Phase

Failures during this stage of interaction mean that the crew did not perform the action correctly given that the previous two stages were correct (i.e., plant status was assessed correctly and the response plan is correct). Included within this phase are the following CFMs:

- E-1: Delay implementation
- E-2: Critical data not checked with appropriate frequency
- E-3: Fail to initiate execution
- E-4: Fail to execute simple response correctly
- E-5: Fail to execute complex response correctly

For each of the CFMs within this stage, an important consideration is concern about timing in implementing the action, given the time available is in principle sufficient, mainly as it impacts the opportunities for and the feasibility of recovery. Although it is within the Action phase that the

error may be manifested, the macrocognitive functions of Sensemaking/Understanding and Decision making are also relevant.

C.1.3.1 E-1: Delay Implementation

For this CFM, the crew has formed the correct plant status assessment in terms of understanding the nature of the plant disturbance and the critical safety functions that need to be controlled or restored; however, the crew delays the implementation of the action to the extent that the response is not successful (i.e., the HFE occurs). This CFM is applicable when the response requires initiation of some action at or before a critical point (may be dictated by time or by a parameter value) in order to successfully restore a safety function.

A couple of reasons may lead the crew to delay implementing the appropriate action. First, competing demands may be viewed as more important at the time. Second, the crew may believe that the respective function can be achieved by recovering a system that normally performs that function without resorting to the action (e.g., believing AFW can be restored in time to prevent going to feed and bleed). Therefore, the crew may believe that they are on the brink of success with an alternative approach and that they have enough time to try these alternative approaches. Table C.1-8 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM. An additional PIF that is considered relevant for this CFM but is not included in the table below is resource limitations resulting from a high workload (may be temporary limitations) that can cause distraction.

Table C.1-8. Relevant PCs, Cognitive Mechanisms, and PIFs for Delay Implementation

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Understanding/ Sensemaking	All	N/A	N/A	This CFM assumes that the correct data is presented and the crew has formed the correct plant status assessment. The error occurs in the decision making process and choosing to delay the correct course of action. Therefore, this PC is not relevant.
Decision Making	Incorrect goals or priorities set	Goal conflict	Procedures Experience Training System response Perceived decision impact (awareness of economic consequences)	This CFM may occur if the crew selects the wrong goal to work toward. A variant of this failure mechanism is if the operator selects an implausible goal that cannot be achieved. Errors may also occur if more than one goal is attempted and the goals are ordered incorrectly in the crew's mind or given the wrong priority, such that less important goals are addressed first. Finally, a conflict may arise in the crew's mind between the goals of safety and the continued viability of the plant.
		Incorrect goals selected	Experience Training Time load	
		Incorrect prioritization of goals	Experience Training Resources Procedures	
	Incorrect internal pattern matching	Not updating the mental model to reflect the changing state of the system	Training Procedures	A possible cause to the error made by the crew is an incorrect estimate of the amount of time available to implement the solution. As the situation evolves, the crew may not properly update their mental model of the plant status and feel they have more time available than they actually have.
	Incorrect mental simulation or evaluation of options	Inaccurate portrayal of the system response to the proposed action	Experience Training Procedures Available and perceived time	This CFM may be due to the crew incorrectly predicting how the system will respond to the proposed action. The crew may believe they have adequate time available to implement the solution in a certain manner or have time to try alternative solutions first. The cognitive bias of overconfidence may also be to blame in causing this CFM. 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.
		Cognitive bias (overconfidence)	Experience Training	

C.1.3.2 E-2: Critical Data Not Checked with Appropriate Frequency

This CFM describes an error made when data that is critical to ascertaining the plant status is not monitored or checked frequently enough so that a cue (e.g., a specific parameter value) for the initiation of a required response is missed. A contributing factor to this CFM is the crew having an incorrect understanding of the rate of change of the parameter such that the

monitoring strategy is deficient. An incorrect understanding of the rate of parameter change is reflected in an incorrect mental model of the plant state and is one of the driving factors in the selection of relevant PCs and cognitive mechanisms. However, this CFM may also occur due to the crew being distracted away from an adequate monitoring strategy. Table C.1-9 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-9. Relevant PCs, Cognitive Mechanisms, and PIFs for Critical Data Not Checked with Appropriate Frequency

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Detecting/ Noticing	All	N/A	N/A	Detection of information is not an issue because the crew knows where to go and knows what needs to be monitored, they just don't do it often enough.
Understanding/ Sensemaking	Incorrect data used to understand the situation	Incorrect/ inappropriate/ inadequate frame used to search for, identify, or **attend** to information	Knowledge/ experience/ expertise Training	For this PC, the detail of having incorrect data may be due to the information itself being faulty, there being errors in the perceptual process (which would direct the problem to the detecting/noticing phase), or the person attending to inappropriate information or focusing on inappropriate aspects of the information. The first and second reasons are not relevant for this CFM as it is not a case that the data is itself faulty or that there are perceptual errors. Instead, the issue lies with the operator having an incorrect frame or mental model which doesn't correctly specify checking information often enough. Furthermore, if the operator misunderstands the rate of change of the parameter, this misunderstanding could lead to an inappropriate monitoring strategy.
	Incorrect integration of data, frames, or data with a frame	Working memory limitations impair processing of information	Working memory capacity Knowledge/ experience/ expertise Training HSI Workload Situation complexity	Within this context, the operator is presented with the correct data and his/her frame or mental model is correct; however, the integration of data, matching of data to frame, or updating process (for updating the frame with the data) goes awry. Specific for this CFM, a mismatch with expectations may lead the crew to an inappropriate monitoring strategy. Alternatively, the cognitive capacity of the crew or operator may be over-taxed such that only a limited amount of the situation is processed. A final alternative is the crew may be distracted away from checking the information with the appropriate frequency.
		Mental manipulation of the information (including projection of future status) is inadequate, inaccurate, or otherwise inappropriate	Knowledge/ experience/ expertise Training	
		Improper control of attention	Knowledge/ experience/ expertise Training HSI	

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
			Workload	
	Incorrect frame used to understand the situation	Incorrect or inadequate frame/mental model used to interpret/integrate information	Knowledge/ experience/ expertise Training Motivation	The crew has a model of the development of the plant status that differs from reality. The changes are occurring quicker than they think they are. An incorrect/incomplete/improper frame or mental model is used to understand the situation.
		Incorrect or inappropriate frame used to search for, identify, or **attend** to information	Knowledge/ experience/ expertise Training	
Decision Making	Incorrect internal pattern matching	Not updating the mental model to reflect the changing state of the system	Training Procedures	A failure occurs because the operator did not correctly update the mental model.
	Incorrect goals or priorities	N/A	N/A	This CFM refers to the understanding of the data; therefore, it primarily takes place within the macrocognitive phase of Understanding/Sensemaking. Planning a response and evaluating alternative solutions (stages within decision making) have not been considered yet.
	Incorrect mental simulation or evaluation of options	N/A	N/A	

C.1.3.3 E-3: Fail to Initiate Execution

This CFM represents the classic error of omission in which the crew fails to initiate a needed response. This CFM is probably best characterized as a lapse, i.e., forgetting to begin the response. Table C.1-10 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-10. Relevant PCs, Cognitive Mechanisms, and PIFs for Failure to Initiate Response

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Action	Failure to execute desired action	Working memory failure	Knowledge/ experience Task load Available time	The most likely drivers to this CFM are forgetting and distraction. High task demands and workload increase this likelihood. Distraction by an increased task load can also cause the action to go uncompleted. Expertise in prioritizing actions and ability in dealing with similar workloads and tasks loads may aid the crew in dealing with these issues. Furthermore, the design of the HSI may either help or hinder the crew as salient cues from the HSI or routine reminders may help to reduce the failures.
		Prospective memory failure	HSI Memory load Task load Available time	
		Divided attention	Task load Available time	
	Execute desired action incorrectly	N/A	N/A	This PC refers to errors of commission whereas this CFM refers to errors of omission.

C.1.3.4 Fail to Correctly Execute Response (E-4: Simple and E-5: Complex)

This CFM describes the situation in which the crew fails to execute the response as required which results in the occurrence of a HFE. It is assumed that the response has been initiated, but then something occurs such that it is not completed correctly. There are a number of ways of failing to perform a response correctly that include not completing all the required actions in time, performing some of the steps incorrectly, or performing the steps out of sequence when the order is critical. This CFM, therefore, is a broader class than the previous CFM and includes both errors of omission and the potential for errors of commission.

For this CFM, three decision trees were constructed to represent simple actions, complex actions, and control actions. Each of these actions has different characteristics making it more suitable to be modeled separately. For instance, continuous, control actions (e.g., cooldown and depressurization following a curve for the pressure and temperature) involve a continuous evaluation of the plant status and making adjustments as necessary. This task, therefore, involves potentially more cognitive activity. Because the nature of the tasks is different, it was useful to develop different trees to address the different cases. Specifically, the three decision trees developed for this CFM are:

1. Failure to correctly execute response – simple task
2. Failure to correctly execute response – complex task
3. Failure to correctly execute response – control action

Most important for the determination of this CFM are concerns about timing in implementing the action (given that the time available is, in principle, sufficient) mainly as it impacts the opportunities for and the feasibility of recovery. Additional PIFs that are prevalent to this CFM include HSI, training, task load and system feedback. The particular aspects of these PIFs that can lead to errors vary with the cognitive mechanism. However, rather than model each of the

cognitive mechanisms explicitly for each of the actions included within this CFM, the approach here is to take these characteristics as a group and use them to identify the characteristics of a task that make it more likely to be error prone. For example, consider the mechanism “dual task interference”. The discussion indicates that this is a potential concern if the operator is performing more than one task at once. Therefore, if the operator is only focused on the (one) task at hand, this mechanism can be considered not to be relevant.

Based on an assessment of the cognitive mechanisms for the Action macrocognitive function (focusing particularly on the proximate cause “Executed Desired Action Incorrectly”), the following are suggested as potential characteristics that need to be addressed:

Nature of response:

- Simple manipulation
- Complex series of manipulations
  - Linear series where ordering does not matter
  - Series where ordering matters (particularly if it leads to an unrecoverable condition)
- Control actions (e.g., depressurization following a curve) – this could be another case of a complex series of manipulations, although it is one in which continuous corrections are expected.

Nature of manner of execution:

- Following a step by step written procedure
  - Does it include checking/verification steps at each manipulation?
- Memorizing a number of steps
  - Does training stress checking/verification?
- Relying on skill of the craft

Nature of feedback:

- Immediate and clear
  - Indicator light changes color, for example
  - Plant parameter value stabilizes (or stops changing) or changes
- Delayed and on completion of the whole task
  - Following completion of steps, task requires verifying that flow has been established, for example. This recovery is more complex since it could involve revisiting the whole series of manipulations.

HSI:

- Well-designed with no issues
- Unique challenging scenario specific issues

Training:

- Needed as a compensatory factor for complex cases
- Stresses checking as a continuous activity

C.1.4 CFMs that Represent Multiple Phases

There are two CFMs that may occur in multiple stages of the crew interactions with the plant. “Misread or Skip Step in Procedure” may occur during either response planning or during execution. “Critical Data Miscommunicated” may occur during any of the three phases and may contribute to any of the other CFMs.

C.1.4.1 AP-1: Misread or Skip Step in Procedure

This CFM deals with slips and lapses in following a procedure and occurs when the operator or crew simply misreads or skips a step in the procedure. In these cases, the information in the procedure is clear and unambiguous; therefore, the error is not due to complexity within or poor writing of the procedure. PCs identified as being relevant to this CFM involve either skipping a step in the procedures or misreading the procedures. Generally a crew may be led to misread or skip a step in the procedures because of a lapse caused by distraction or forgetfulness. The error is, therefore, unintentional and is driven by the workload, procedural complexity and time pressures. In general, training, knowledge and experience are not considered to be drivers for this CFM. It is assumed that the training for the operators in reading the procedures is adequate. The issue here is a slip or lapse in reading the procedures that is not driven by either a lack of knowledge or an incorrect mental model of the plant system. However, training may be seen as a compensatory factor on how well the operators handle multiple tasks competing for their time and attention. Table C.1-11 presents a discussion of those PCs, cognitive mechanisms, and PIFs that were evaluated as being relevant to this CFM.

Table C.1-11. Relevant PCs, Cognitive Mechanisms, and PIFs for Misread or Skip Step in Procedure

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Detecting/ Noticing	Cue/information not perceived	Vigilance in monitoring	Task complexity Task load Attention Stress	Both of these PCs are relevant to this CFM in that they describe ways in which a procedure step may be skipped when considering the procedure step is a cue or type of information. The information (i.e., procedure step) may either not be perceived or not be attended to.
		Working memory	Task load	
	Cue/information not attended to	Vigilance in monitoring	Loads Stress Attention Task complexity Fatigue	
		Working memory	Task load Training	
	Cue/information misperceived	N/A	N/A	The step in the procedure is not misperceived (as described in this PC), it is missed completely.
Understanding/ Sensemaking	All	N/A	N/A	This CFM deals with missing the information presented in the procedure step completely; therefore, making sense of the procedure or integrating the information into the mental model is not addressed here.
Decision Making	All	N/A	N/A	It is not a conscious decision to skip or dismiss a step in the procedures. Instead, the error is simply a slip or lapse and does not deal with the decision making process.
Action	Failure to execute desired action	Divided attention	Task load Non-task load Available time	This PC is relevant if the "desired action" is interpreted to mean executing the step in the procedure. Because the step is skipped, the action is not executed.
	Execute desired action incorrectly	Dual task interference	Task load Non-task load	This PC is relevant to the CFM in that it explains why a procedure

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
			Available time	may be misread. Therefore, the desired action that is being executed incorrectly is the reading of the procedure.
		Task switching interference	Task load	
			Non-task load	
			Available time	
		Negative transfer/habit intrusion	Task load	

C.1.4.1 C-1: Critical Data Miscommunicated

For this CFM, critical data is unintentionally incorrectly transferred between crew members. In this context, data could be an instruction as well as a parameter value or a report on the status of a function, system or component. The error committed is unintentional, therefore, the error primarily manifests as a slip. The failure scenarios that result from this CFM tree include both the failure that results in directing a crew member to obtain incorrect information (e.g., data from the wrong train), and the transference of the incorrect data to the procedure reader and decision-maker. A third instance could occur in which the correct data is communicated, but it is not heard due to either distractions or other environmental factors (e.g., high noise). In this context, data could in fact be an instruction rather than a parameter value.

The proximate cause relevant to this phase of interaction is exclusively “Failure of Team Communication” within the macrocognitive function of Team Coordination. The other PC within that macrocognitive function is “Error in Leadership/Supervision”, and that PC was determined to not be relevant due to the inability to evaluate such aspects at this level of HRA. The PIFs related to external influences such as the environment, proximity, and (communication) equipment were added; they were not specifically identified in the psychological literature search as they are not cognitively driven but are generally accepted as influencing communication effectiveness.

For the target error of commission, one of the cognitive mechanisms was postulated to be an incorrect integration of the information with a mental model. The literature review table of crew coordination gives an example where the target is expecting the source to ask for something different from what he/she actually asks for, but the target interprets the request according to his/her expectations. Trying to model down to this level of detail was determined to be too complicated and unnecessary at this stage. If desired, a more detailed model of the crew interactions could be developed. This level of detail could, for example, result in the identification of more opportunities for crew self-correction such as the target of the information matching it to his/her mental model and realizing it does not fit and, therefore, requesting confirmation. However, lacking a more complete crew interaction model, this CFM is used primarily to address failures in the mechanics of communications.

Table C.1-12 presents a discussion of the cognitive mechanisms and PIFs that were evaluated as being relevant to this CFM.

Table C.1-12. Relevant PCs, Cognitive Mechanisms, and PIFs for Critical Data Miscommunicated

Macrocognitive Function	Proximate Cause	Cognitive Mechanism	PIF	Discussion
Team Coordination	Failure of team communication	Source error of omission	Time pressure Resource management	The error may occur either due to the source of the message either failing to communicate the correct message or communicating it incorrectly (source error of omission or commission). Alternatively, the error may be due to the target either not hearing the message or hearing it incorrectly (target error of omission or commission). These errors may take place due to, for example: 1) the crew member may have been directed to collect the wrong information 2) the right information was collected but communicated incorrectly, 3) the information was spoken correctly but was misheard. For this CFM, the information is correct, but either the target or the source gets it wrong.
		Source error of commission	Knowledge/ experience Training Task complexity	
		Target error of omission	Environment (e.g., noise, the need to wear SCBA) Task load Training (on communication protocol) Proximity (between source and target) Equipment	
		Target error of commission	Knowledge/ experience Environment (e.g., noise, the need to wear SCBA) Task load Training (on communication protocol) Proximity (between source and target) Equipment	

C.2 Cognitive mechanisms and PIFs

This section provides the completeness checking on the cognitive mechanisms (identified in NUREG-2114) represented by the PIFs in the DTs. Each CFM is linked to the relevant Proximate Causes (PCs). For every relevant PC, we evaluated all the identified cognitive mechanisms against the PIFs (i.e., DT branches) to determine whether the DT captures the mechanisms. We performed a mapping between the cognitive mechanism and the DT branches. The mapping is annotated as follows:

1. Most cognitive mechanism were captured fully or partially by one or more of the PIFs (DT branches)
2. The mechanism is NOT APPLICABLE to the CFM being described. For example, the mechanism "Overreliance on primary indicator" is not applicable to the CFM "Key alarm not attended to" because the key alarm is the primary indicator.
3. The mechanism is NOT SIGNIFICANT to the CFM for procedure-based actions in internal at-power events. Although the mechanism is theoretically applicable to the CFM, its impact is nominal or negligible given the assumptions of IDHEAS quantification model (well experienced crew, well trained procedures, and reasonable good control room HSI).

Regarding item 1), notice that even if one or several PIFs of a DT are linked to a mechanism, the scope of the PIFs may only represent a subset of the ways or characteristics that challenges the mechanism. The IDHEAS development team selected the PIFs that are most relevant to procedure-based actions in internal at-power events. For example, for the CFM "Key alarm not attended," the mechanism "Cue salience is low and not detected" is mapped to the PIF "HSI - Is the alarm (or pattern of alarms) prominent, distinctive and unambiguous?" Yet, the same mechanism can also be challenged by noise, ambient light, or other environment factors. The noise factor was not selected because it was assumed that the crew's work location is very close to alarms therefore the impact of noise is minimal. This justification may not be valid for external events such as flood or earthquake.

The table below presents the cognitive mechanisms that were considered as NOT SIGNIFICANT (NS) or NOT APPLICABLE (NA) as well as the justification for every CFM. A brief description of the PIF scopes for every CFM is provided.

Table C.1-2: Cognitive mechanisms that are not represented by the decision-trees

AR – Key alarm not attended **Workload** - whether, for the PRA scenario, the cognitive workload is higher than that which is considered normal and for which operators are well trained. **HSI -** Is the alarm (or pattern of alarms) prominent, distinctive and unambiguous? Is the alarm or pattern of alarms discernible from the background noise generated by coincident alarms/information and is its relevance evident? Can the target for response be unambiguously and readily identified, and is its manipulation consistent with practice (i.e., no non-stereo-typical or unintuitive actions)? **Perceived Urgency/Significance** - whether the training and experience of the crew emphasizes the significance of the alarm and the required response such that the operators are conditioned to recognize and prioritize the alarm.			
Proximate causes (PC)	**Cognitive mechanism**	**NA or NS**	**comment**
Cues/information not perceived	Unable to maintain vigilance	NS	CR alarms are salient and CR crews are assumed in good vigilance for internal at-power actions.
Cues/information not attended to	Overreliance on primary indicator	NA	Key alarms are the primary indicators for crew to rely on
Cues/information misperceived	Cognitive bias on expectation	NS	Expectation should not play a role because it is an unexpected alarm

SA-1: Data Misleading or Not Available

Alternate/Supplementary Source of Information - whether, given the primary cue or source of information is either failed or misleading, there are alternate indications that could be used to obtain the plant status

Information Obviously Incorrect - whether the primary information is obviously incorrect or ambiguous

Guidance to Seek Confirmatory Data - whether there is guidance that would lead the crew to consult the alternate sources of data and the nature of that guidance

Distraction - whether there is something (e.g., high workload and insufficient time) that results in distraction such that the likelihood of obtaining the correct information from the alternate sources is lessened.

PC	Cognitive mechanism	NS or NA	Justification
Cues/information not perceived	Cue salience is low and not detected	NS	CR design makes this unlikely
	Unable to maintain vigilance	NS	CR crew are assumed to have good vigilance
	Working memory capacity overload	NS	CR crew has procedures aiding their working memory
Incorrect data (for Understanding)	Attention to wrong or inappropriate information	NA	The CFM is about attending to or selecting improper data
	Improper data or aspects of the data selected for comparison with or identification of a frame	NA	Same as above
	Data not properly recognized, classified, or distinguished.	NA	This is the outcome of the CFM

Note: This CFM has as a premise that the data available to the operators has been obtained and correctly understood. The problem is that the data is incorrect. This CFM is really looking at whether there are sources of information that can provide the correct data: whether there is guidance to do so; and whether they are in a high workload situation.

Therefore, the CFM has less to do with cognitive mechanisms than it does with determining whether there is a chance of compensating for a bad (misleading) piece of data. The cognitive mechanism aspect is more of a second order effect and is really captured in the last question, workload, which we used as a surrogate for all the ways they could fail to implement the recovery available to them

SA-2: Wrong Data Source Attended to

HSI - whether there is potential for the target source of data to be confused with another

Workload - Is the crew member responsible for obtaining the data also responsible for other coincidental tasks, or is the task complex (in the sense of requiring a number of different activities within a relatively short time)?

Familiarity with the data source - whether the training and the experience of the crew makes it unlikely that the wrong source would be attended to

PC	Cognitive mechanism	NS or NA	Justification
Attention to wrong/inappropriate information	Cue salience is low and not detected	NS	This CFM pertains to a directed search for information. Salience is not the problem here – a piece of data has been obtained and understood, it's just that it's the wrong piece of data.
	Unable to maintain vigilance	NS	CR crew are assumed in good vigilance (complying to fitness-for-duty)
Attention to wrong/inappropriate information	Overreliance on primary indicator	NS	This CFM pertains to a directed search for information

SA-3: Critical Data Misperceived

HSI/Environment - whether the information source can be difficult to interpret for the subject scenario.

Workload - The number and/or nature of the activities that the person responsible for collecting the data is performing at the time the data is to be collected

Training- level of training and experience the crew has with a specific scenario or indicator.

PC	Cognitive mechanism	NS or NA	Justification
Cues/information not perceived	Unable to maintain vigilance	NS	CR crew meets fitness-for-duty

SA-4 Critical Data Dismissed/Discounted

Valid Alternative/Deviation Scenario – Whether there a plant signature that, with the collection of the critical information dismissed, is an anticipated plant state.

Bias - whether a bias from training and knowledge/experience/expertise with respect to the plant status could affect the crew's behavior

Indications Reliability - the crew's perception of the reliability of the information that is being dismissed,

Confirmatory Information - Are there additional indications that would typically be used to confirm the plant status indicated by the information

PC	Cognitive mechanism	NS or NA	Justification
Incorrect data	Attention to wrong or inappropriate information	NA	The CFM is about dismiss data attended
Incorrect frame	No frame or mental model exists to interpret the information or situation.	NA	This is a case that is clearly outside the procedures and training, and would correspond to an analytical process based on incomplete knowledge.
	No frame or mental model exists to interpret the information or situation.	NA	This is a case that is clearly outside the procedures and training, and would correspond to an analytical process based on incomplete knowledge. .
Incorrect integration of data and frame	Working memory limitations impair processing of information	NS	The use of procedures mitigates working memory load - this CFM refers to a deliberate choice to dismiss a piece of information because by doing so they have a viable plant status, This implies that the working memory capacity is sufficient for that purpose.

SA-5: Premature Termination of Critical Data Collection

Viable Alternative Plant Status Believable - whether, in the absence of the critical data that is the subject of this CFM, but with all the data pertaining to the plant status taken into account, there is a plant status that is valid and within the spectrum of plant conditions that is encompassed by knowledge base of the crew.

Expectations or Biases – Addresses whether a bias from training and knowledge/experience/expertise could cause the crew to form a mental model of the plant status prematurely.

Workload – This assesses available time, number of simultaneous tasks and available manpower.

HSI – This refers to the clarity and ease of access to the indications that provide the data

PC	Cognitive mechanism	NS or NA	Justification
Incorrect data (for Understanding)	Information available in the environment (including procedures) is not complete, correct, or otherwise sufficient to create understanding of the situation	NA	The mechanism already addressed by another CFM (SA-1)
	Attention to wrong or inappropriate information	NA	The CFM is more of a deliberate inattention to the right data.
	Improper data or aspects of the data selected for comparison with or identification of a frame.	NA	this is really evaluated first on whether there is a viable plant status if they terminate collection of the critical data, then understanding whether the training biases their actions
Incorrect frame	No frame or mental model exists to interpret the information or situation.	NA	Unlikely for CR actions in internal at-power events - In this case, the

			frame does exist to justify the action taken to terminate collection, so it is certainly inapplicable.
Incorrect integration of data and frame			

RP-1 Misinterpret procedures

Procedure Open to Misinterpretation - whether a single step or group of steps may be easily misinterpreted to put operators on a failure path.

Workload - whether there are coincident tasks or time pressure that act as exacerbating factors

Training - whether there is specific training and/or experience on the scenario help to address holes in the procedures or areas that might lead to confusion.

PC	Cognitive mechanism	NS or NA	Justification
Incorrect Goals or Priorities Set	Goal conflict. A conflict may arise in the operator's mind between the goals of safety and the continued viability of the plant.	NA	Procedures for CR-actions avoid goal conflicts
	Incorrect prioritization of goals. Goals may be ordered incorrectly in the operators' mind or given the wrong priority, such that less important goals are addressed first.	NA	Same as above
	Incorrect judgment of goal success	NA	Same as above
Incorrect Internal Pattern Matching	Cognitive biases. Confirmation bias and availability bias may be particularly pertinent to causing errors in this phase of decision making	NS	Crew follows procedures
Incorrect Mental Simulation or Evaluation of Options	Inaccurate portrayal of action. This failure mechanism includes incorrectly characterizing the action (i.e., forgetting a step of the action during the mental simulation) or incorrectly predicting how the action will be implemented.	NS	Procedures validated the options
	Cognitive biases. The cognitive biases of overconfidence and the anchoring effect may be especially prevalent for this failure mechanism. Overconfidence affect	NS	Crew adheres to procedures

RP-2 Choose inappropriate strategy

Preference for Correct Strategy – Whether the crew has a strong preference to choose the incorrect option over the correct alternative because of training, experience, or perception of response complication

Advantage to Correct Strategy - whether there are considerations related to the correct response that interfere with the operators choosing that response, such competing priorities, downside to the correct option, or mismatch between the procedures, policies and practice.

PC	Cognitive mechanism	NS or NA	Justification
Incorrect Internal Pattern Matching	Not updating the mental model to reflect the changing state of the system.	NS	Procedure based decision-making - This is applicable when the procedure provides more than one success path but doesn't say which to use.
	Cognitive biases.	NS	Crew adheres to procedures
Incorrect Mental Simulation or Evaluation of Options	Inaccurate portrayal of action - incorrectly characterizing the action or incorrectly predicting how the action will be implemented.	NS	Actions are procedure-based
	Incorrect inclusion of alternatives. The operator may forget to include some alternatives that should be considered.	NS	Procedures provide alternatives
	Inaccurate portrayal of the system response to the proposed action.	NS	Unlikely for internal at-power events

E-1 Delay implementation

Reluctance and Viable Alternative - whether there could be a reason for the operators not to want to perform the response as required.

Assessment of Margin - whether the crew has an incorrect assessment of the operational margin (e.g., as measured or indicated by pressure, level, temperature) so that they think they can delay implementation longer than they actually can.

Additional Cues - whether there are additional cues that act as a potential recovery to refocus the crew on the need to begin the execution expeditiously.

PC	Cognitive mechanism	NS or NA	Justification
Incorrect Goals or Priorities Set	Incorrect judgment of goal success	NS	Judgment is assumed in procedures
Incorrect Internal Pattern Matching	Not updating the mental model to reflect the changing state of the system.	NS	Procedure-based decision-making
	Cognitive biases. Confirmation bias and availability bias may be particularly pertinent to causing errors in this phase of decision making	NS	Crew adheres to procedures
Incorrect Mental Simulation or Evaluation of Options	Incorrect inclusion of alternatives. The operator may forget to include some alternatives that should be considered.	NA	

E-2 Critical Data Not Checked with Appropriate Frequency

Monitoring Optimized - Whether a crew member assigned to watch the key parameter or whether are the operators trained on how to adequately monitor the key parameter.

Importance of Data Understood - Whether the operators are trained on the significance of the parameter so that the monitoring task is given priority over other tasks he may have to perform, or at least to check the parameter frequently

Match with Expectations - whether the training and experience of the crew are sufficient to establish an appropriate monitoring regime.

Alarm - the alarm is considered as a reminder that the critical level of parameter has been reached

PC	Cognitive mechanism	NS or NA	Justification
Failed to take required action	Working memory failure		Unlikely for CR actions
	Prospective memory failure		Same as above
Cues/information not attended to	Overreliance on primary indicator	NA	

E-3 Fail to Initiate Response

Immediacy - Whether operators are trained to respond for the scenario in question, and in particular, to identify if this is an immediate action.

Workload - whether there is a distraction caused by high workload

PC	Cognitive mechanism	NS or NA	Justification
Failed to take required action	The three cognitive mechanisms (Working memory failure, Prospective memory failure, and Divided attention) were represented by the PIFs.		

E-4 Execute simple action incorrectly

HSI - The aspects of HSI that are considered in this branch are those that have a direct impact on the performance of the response (i.e., task-specific HSI, not general plant HSI), and will include the indications and controls relevant to the response. If there is good training on this indicator, the HSI can be considered GOOD.

Workload - Workload refers to anything that might distract attention from the task such that there is an increased chance of it being performed correctly. High workload includes competing tasks and time pressure.

PC	Cognitive mechanism	NS or NA	Justification
Failed to take required action	Working memory failure	NS	Actions are based on procedure steps
	Prospective memory failure	NS	Actions are based on procedure steps
Executed desired action incorrectly	Error monitoring and correction	NS	Not important for simple action
	Negative transfer/habit intrusion	NS	Not for well-trained crew in CR
	Automaticity control	NA	Actions are based on procedure steps
	Mode confusion	NS	Unlikely for CR HSI design
	Population stereotypes	NS	Not for well trained crew
	Motor learning	NS	Crew trained and qualified for performing the motor movements of the actions

E-5 Execute complex action incorrectly

Execution Straightforward – One of the following situations: a) The task does not require skillful coordination of multiple manipulations. **b)** The task may be completed at a reasonable pace with ample opportunity for checking instead of having to be done expeditiously. **c)** There are no steps that if reversed could cause a failure of the response (e.g., by damaging equipment). **d)** There is nothing unusual or inherently difficult about the tasks that would normally cause any problems for those executing the actions.

Training - whether training is sufficient to minimize the opportunities for error for tasks with some inherently complex aspects.

Work practice - Whether, either as a result of standard work practices or by procedure, there are factors that enhance the likelihood that the task, even though complex, can be performed reliably.

PC	Cognitive mechanism	NS or NA	Justification
Failed to take required action	Working memory failure	NS	Use of procedures
	Prospective memory failure	NS	Use of procedures
	Divided attention	NS	Minimized by CR peer-checking and supervision
Executed desired action incorrectly	Automaticity control	NS	Use of procedures
	Mode confusion	NA	CR HSI does not have mode confusion
	Population stereotypes	NS	Trained crew
	Motor learning		Crew trained and qualified for performing the motor movements of the actions

Appendix D. Expert Judgment of HEP Distributions for IDHEAS Decision Trees

D.2 Objective of the Expert Elicitation (EE)

The objective of the EE was to obtain estimates of the HEPs to be used in the IDHEAS quantification model based on inputs from a number of experts using supporting data. The eventual outcome of the EE included 1) HEPs for the each of CFMs for the range of contexts implied by the paths through the decision trees and 2) experts' opinions about the strength of the effects of PIFs on given CFMs that could be used to guide determination of HEPs both during the elicitation and afterwards, when the Technical Integrator (TI) completed the assignment of HEPs to all paths through the DTs (this process is discussed further below).

The Scope of the EE was limited to the following:

1. The HEP estimates are based on conditions assumed for internal at-power events;
2. Only the HEPs of a subset of all the DT paths for each CFM were elicited (due to time and resource limitations) at the EE workshops. After the workshops were completed, the evaluator experts (discussed below) completed assignment of HEPs to a subset of the DT paths for each CFM and provided these results to the TI, who then completed assignment of consensus HEPs to all paths for which there was adequate consensus.

D.3 The SSHAC method for obtaining expert judgment

Given that there is limited direct data that could be used for HEPs, and estimating HEPs requires expertise in multiple areas such as NPP operation, HRA/PRA, human performance, and cognitive psychology, interaction among experts from different areas is necessary. Thus, we choose the SSHAC process. SSHAC emphasizes three aspects: 1) thorough collection and investigation of data that can be used to support judgments; 2) interactions among the experts to maximize available experience and knowledge, and sharing and assessment of the information; 3) use of a TI and peer reviewers to minimize biases in judgment during the process and facilitate decision-making.

The basic assumption for SSHAC process is that experts need to develop or select a model on which the judgment is based. In our case, the IDHEAS team has already developed the model (the CFMs and DTs). Thus, we simplified the process by focusing on assessing the available data, eliciting experience/expertise, and making HEP estimations based on the experts understanding of the available information and their own experience. SSHAC guidance relies on proponent experts to propose models of their judgment on whatever is being assessed. In our process, since the HRA model has already been proposed, the proponent expert described the HRA model (IDHEAS) and the underlying structure for the items being elicited from the evaluator experts, in this case, the HEPs. The technical integrator(s), using their experience in PRA/HRA and nuclear power plant operation, and the data and information provided by the data and resource experts, provided the expert opinion on what the HEPs should be. The resource experts provided their knowledge and expertise in cognitive psychology, plant operation and operator performance, and human event analysis to the proponent experts to support the expert opinions being elicited. The data-team provided the empirical data associated with CFMs and PIFs.

D.3.1 Selection of SSHAC Level

Following the SHACC guidance for selecting the level of the expert elicitation, a modified, SSHAC Level-3 process was selected in which resource/proponent experts interact with evaluation experts in facilitated workshops to obtain the desired expert opinions. The Level-3 process emphasizes the interaction among the experts in facilitated workshops using a TI to ensure the high-level confidence in the outcome.

D.3.2 Project Organizational Structure

SSHAC Level-3 uses the following organizational structures:

- Project Manager(s) - Manage the project, coordinate the activities, ensure that workshops focus on the agenda and move forward according to the schedule, and facilitate the workshops, responsible for the production of the final report.
- Data team - The role of the data team is to collect and organize data/information/evidence proponent experts to support the EE.
- Resource experts - The *role* of a resource expert is to present data and knowledge in an impartial manner. The main responsibility of a resource expert is to share their technical knowledge and judgment relevant to the EE in an impartial way in their presentations to the proponent experts. This means that their presentation should make full disclosure including all caveats, assumptions, and limitations. The resource experts are expected to respond candidly and impartially to questions posed by the proponent experts. They also fill out worksheets that document their knowledge and judgment. Six resource experts participated in the project: One cognitive psychologist who is also an IDHEAS developer, three operator trainers with SRO experience, two NRC reliability engineers who perform and review HRA in SDP/ASP programs, and one industrial PRA analyst who is the main developer of IDHEAS quantification model.
- Proponent experts - The responsibility of a proponent is to develop and promote the adoption of his or her model/justification/judgment of HEPs. . The proponent is required to justify this assertion, to demonstrate the technical basis for the model/judgment, and to defend the model/judgment in the face of technical challenge. The five proponent experts at each workshop were a mixture of operator trainers and HRA/PRA analysts and proponent experts Lead Technical integrator (TI). The main roles of the TI include proponent experts facilitating the workshops and integrating the estimation made by the proponent experts. The main attributes of a TI are the ability to objectively evaluate the views of others in developing HEPs and control for potential bias so that each expert has the opportunity to bring their evidence to the table and freely express their views. The TI is the key decision-maker in integrating diverse or controversial judgments among the TI members and for this EE, will integrate the HEP information from the evaluator experts to determine the HEPs and where gaps exist, will extrapolate the available information to provide HEPs for failure paths that could not be addressed by the entire team of proponent experts due to time and resource limitations.
- Peer reviewers (PR) - The PR fulfills two parallel roles, the first being technical review. This means that the PR is charged with ensuring that the full range of data, models, and methods have been duly considered in the assessment and also that all technical decisions are adequately justified and documented. The second role of the PR is process review, which means ensuring that the project either conforms to the requirements of the selected SSHAC process level or deviate from the standard

SSHAC process with justification. Collectively, these two roles imply oversight to assure that the integration is performed appropriately. Two PRs participated in the workshops.

D.4 Process of the Expert Elicitation

Three workshops were conducted to obtain the HEP estimation. Workshop 1 was to review available data and the model (IDHEAS); Workshop 2 was for proponent experts to estimate HEPs; Workshop 3 is a continuation of Workshop 2 to finish the estimation for all the DTs. Since the complete set of HEPs for the DTs could not be obtained during the two workshops, the proponent experts proponent experts completed their estimation by providing HEPs (including 90th, 50th, and in some cases 10th percentile values) for selected decision paths on data sheets and forwarded them to the TI. The TI then integrated the relevant information and completed "consensus" HEP distributions (with the intent of representing the technical community).

D.4.1 Preparation

This section describes the principal work activities that were completed in preparation for the EE workshops.

1. Database development - The data team identified data relevant to human performance and human error under conditions similar to those being addressed for the IDHEAS decision trees. Various sources such as the psychological and human factors literature, human event databases, and simulator data repositories were reviewed and the results were organized into a database and summarized in a format that suited the intended use. The database includes (1) aggregated quantitative data (e.g., HEPs, failure rates, and uncertainty bounds), (2) description of tasks and/or scenarios associated with the quantitative data, (3) PIFs and relevant information identified from the data sources, and (4) data source information. The intent was that the resource and evaluator experts would use this database as a reference and technical basis to support their judgments about the factors contributing to the likelihood of the CFMs and their estimated HEPs given the identified conditions. The resulting database is presented in Attachment 1 below. In addition, a summary of the data for more direct use at the workshops is presented in Attachment 2. Both of these were provided to the various experts prior to the first workshop.
2. Training for the EE workshops – To prepare the various experts for participation in the two workshops, relevant material was sent out to the scheduled participants ahead of time and the material was discussed in a conference call approximately two weeks before the first workshop. Material covered in the call included:
   - A description of the IDHEAS HRA method. A draft of the report documenting the method had been sent to the participants ahead of time.
   - Objectives of IDHEAS expert elicitation
   - A description of the formal expert elicitation method to be used (i.e., SSHAC) and the planned controls for bias.
   - An overview of the purpose, plans, and expected products of the workshops, with an emphasis on the details for Workshop 1.
   - A discussion of an example worksheet (and supporting material) that would be filled-out by the resource experts at the first workshop to identify the key contributors to the likelihood of each CFM (based on the factors addressed in the DTs) and the initial estimates of the likelihood of failure, given the various conditions represented in the DTs. The supporting material accompanying the worksheet included the CFM definition, a scenario example, the DT from the quantification model, and a discussion of the factors addressed in the DT to quantify the CFM. Taken together, this information was referred to as a CFM

Worksheet Package. Such packages were developed for each CFM and provided to the experts prior to the first workshop. An example worksheet package is provided in Attachment 3. This information was discussed in detail for each CFM at the first workshop.

3. Development of Materials and Review for the Workshops – The main material developed specifically for the first workshop was the CFM Worksheet Packages (see above). As is described below under Workshop 1, the resource experts were those responsible for filling out the worksheets for the first phase of the EE. These experts were encouraged to review and initially fill out as many of the worksheets as possible before the first workshop. These worksheets were completed by the resource experts during and after the first workshop. Based on the feedback and results provided by the resource experts and other participants from the first workshop, revisions were made to some of the CFMs, DTs and associated elements of the quantification model and the new material was provided to EE participants for the second workshop. Documentation of the changes that were made was provided to the participants and new worksheets for the proponent experts to document their HEP estimates were also provided.

D.4.2 Workshop 1

In addition to familiarizing all participants involved in EE with the supporting empirical database and the key elements and logic of the CFMs, DTs, and PIFs used in the IDHEAS quantification model, the primary purpose of the first workshop was to review available data and IDHEAS quantification model, obtain information from the resource experts about the factors addressed in the DTs used to evaluate the likelihood of failure and obtain their initial qualitative judgment of the HEPs and the contribution of the PIFs to the HEPs for the DT in terms of their relative rankings (very low, low, moderate, or high probability of failure). The resource experts had expertise in several areas proponent experts. The resource experts consisted of individuals with the following expertise:

- Three operator/trainers from three NPPs, including two PWRs and one BWR
- One cognitive psychologist, who also had expertise in HRA
- Two NRC employees familiar with human event analysis, including a staff member from NRR familiar with the NRC significance determination process (SDP) and an RNC licensing examiner

It was thought that the views of these diverse experts on the importance of the factors addressed in the DTs and their inter-relationships and dependencies would provide supporting information and insights to the proponent experts. In addition, it was thought that operational or other types of examples illustrating the aspects being addressed in the quantification model would be extremely useful.

For each given CFM, the expert panel first review and discuss the CFM definition and the DT. The resource experts then filled out their worksheets that includes the relative importance of the various PIFs for the CFMs being addressed, potential dependencies or interactions between the PIFs that could influence their effects, any other PIFs that might be important that had not been included in the DTs, and initial estimates of the likelihood of failure of the various DT paths. These estimates could be simple difficulty rankings (very low, low, moderate, or high probability of failure) or actual HEPs, but guided by a scale that provided ranges of HEPs corresponding to the rankings. In addition, the resource experts were asked to write down any operational examples or other information that would help clarify their opinions. An example worksheet for a selected CFM, along with the type of information that came in each worksheet package for each CFM is provided in Attachment 1.

After the worksheets were completed, each expert presented his or her results and the basis for those results to the participants in the EE. Additional discussion was held as needed to allow participants to understand the resource expert's decisions. Since not all the CFMs could be completed in the three-day workshop, the resource experts completed their worksheets after the workshop and submitted their results within one week. The results from all of the resource experts for each CFM were forwarded to evaluator experts prior to Workshop 2.

It should be noted that the experience of the NPP operators/trainers, in terms of what they had actually seen operating crews doing in simulated accident scenarios and the factors that seemed to influence them the most, provided very useful information. These examples and related information was used to guide revisions to the CFMs, DTs, and PIFs and provided the proponent experts important insights for their judgments in the 2nd workshop. Some of the examples were documented in the EE meeting notes and forwarded to the participants prior to Workshop 2.

D.4.3 Workshop 2 & 3

The ultimate goal of the EE was to produce a consensus distribution showing the 10th, 50th, and 90th percentile values, along with a mean HEP value, for the end point of each failure path in each DT. The consensus distribution was to represent that of the technical community based on the distributions provided by the proponent experts in Workshop 2 and as integrated by the TI. However, as was noted above, the complete set of HEPs and associated distributions for all of the paths through all of the DTs could not be completed during the 2nd workshop. Thus, while as many of the DT paths as possible were completed during Workshop 2, the proponent experts had to complete some of their estimates after the workshop. Their results were then forwarded to the TI to integrate the inputs from the proponent experts into the consensus distributions. The results of this process are discussed and presented in Section D.5.1.

To support the proponent experts as much as possible in working through the process for developing the distributions and to allow the technical exchange of information between the proponent experts as they addressed the various DTs, a subset of DTs and failure paths were selected for the workshop. The idea was that through exchange of information and opinions between the proponent experts (including participation by the resource experts in the discussions) for a subset of the different types of CFMs and associated DTs, the proponent experts would be prepared to continue the exercise on their own after the workshop. Thus, several CFMs from the situation assessment, response planning, and response execution phases, were selected during the workshop. The goal was for the proponent experts, guided by the TI and supported by the resource experts and the results from Workshop 1 as needed, to provide distributions for the best and worst paths through a given DT, along with one or two other selected paths that would provide as good of understanding as possible of the PIFs and how they would affect the probability of failure of the CFM. The TI would then take these results, along with the remaining estimates sent by the proponent experts after the workshop, and produce the resulting consensus distributions and mean HEP value for each of the paths through the DTs.

As in Workshop 1, the proponent expert would first walk all the workshop participants through the worksheet package for a given CFM/DT (in some cases these had been revised based on information from Workshop 1) and the participants (particularly the evaluator experts) could ask questions of the proponent and resource experts and of each other regarding the CFMs, DTs, and PIFs. After the discussion for each CFM, each evaluator would provide their opinions/estimates of the distribution for a selected path

through the DTs and these would be recorded for the group to see. Each evaluator would also provide the rationale for their selected values. After all proponent experts had provided their rationale for their estimates, each was given the option of revising their estimates based on what they had heard from the other proponent experts. There was no pressure for anyone to change their values and the TI was careful to ensure that everyone had a chance to make clear the basis for their opinions. In some cases changes occurred, in others not. When changes did occur, they were noted in the respective worksheet for the given path in a DT tree being addressed.

As noted, the proponent experts completed any of the remaining DT paths that had been planned for the workshop but not completed (e.g., best and worst paths, along with a couple other paths for each DT) after the workshop and forwarded their results to the TI. The TI then took the input from all of the proponent experts and completed the consensus distributions for all the paths through the DT.

D.5 Summary Consensus Distributions

Consensus distributions were developed during Workshop 2 & 3. During the time available, estimates were developed for many contexts. Extensive discussions during the elicitation process provided the TI with substantial information for developing preliminary consensus distributions. Following the workshop, the proponent experts developed additional estimates for many other contexts. The TI developed suggested consensus distributions based on previous discussions and notes provided in the individual evaluator worksheets.

Note that several additional aspects of the EE results were documented, but they are not included in this report. They included 1) the complete set of distributions for each decision tree path (CFM and context) by each proponent expert along with the consensus distribution suggested by the TI, 2) the arguments provided in writing by each evaluator supporting their initial rationale, and 3) details of the discussion that led to revisions in estimates by the individual proponent experts as well as the consensus distributions.

D.5.1 Findings and Conclusions

In summary, he modified SHAAC process worked reasonably well. All participants in both workshops participated fully. Efforts to control bias were largely successful, in that all participants provided their personal evaluations and openly discussed the factors and evidence supporting their initial positions. All willingly listened to other positions and considered them, when working toward consensus. The group tried to discuss the range of informed positions within the technical community. The three workshops worked, as intended, with the first defining the issues and providing the common knowledge base for the elicitation process in the second.

D.5.2 Limitations and Caveats

The TI served as facilitator for the group and performed his own evaluations. That is, he also served as one of the proponent experts in Workshop 2. This presents a potential conflict and source of bias. The TI, the peer reviewers, and the project managers all provided oversight and direction during the meetings to assist in ensuring that this potential bias was controlled.

Not all participants were fully familiar with the IDHEAS methodology and its bases. As discussed further below, this led to some conceptual problems that complicated the elicitation process to some extent.

Two problems limit confidence in the actual 'consensus' distributions: (1) reading materials and the activities of Workshop 1 failed to instill a full appreciation of the meaning of paths through the decision trees and (2) there was insufficient time in Workshop 2 to develop full group consensus distributions for the decision tree paths.

The first problem is rooted in the need to fully understand the IDHEAS methodology. That methodology assesses the contexts under which actions take place, as part of the crew response tree development. That effort would also define the likelihood of that particular context occurring, in light of the actual accident in progress. Our task in Workshop 2 was to evaluate the likelihood of operator failure, given that context. The decision tree is simply a map defining the possible contexts, with each path representing one particular context; the issue of likelihood is not considered in the decision tree. Our task was to evaluate the likelihood of failure, given that the particular context actually exists. Some of the proponent experts had real difficulty maintaining this separation of the problem; that is, they were driven to moderate the probability of failure by their perception of the likelihood that a particular path could exist. We tried to identify this problem, when it occurred, and to adapt the consensus discussion to account for it.

The second problem was the time resource for the workshops. We structured the second workshop to focus first on those CFMs deemed most important to risk calculations and second on the more severe paths associated with each CFM. Even so, we only managed to develop consensus distribution for all or partial DT paths in nine DTs. Following the workshop, the proponent experts submitted estimates for many of the remaining paths in the decision trees. For the cases, where the estimates were in reasonably close agreement and the supporting arguments were clear or there had been useful discussion during the workshops, the TI suggested possible consensus distributions. Finally, there were several DT paths with no consensus distributions. We interpolated their HEPs from the consensus HEPs pf those paths of the same tree.

D.6 Expert judgment of HEP distributions

This section presents the HEP distributions of all DT paths. Each table is for one DT. Notice that the HEP distributions for some DTs were estimated at 5^{th}, 10^{th}, 50^{th}, 90^{th}, and 99^{th} percentiles, while for other DTs they were only distributed at 10^{th}, 50^{th}, and 99^{th} percentiles due to experts' limited time resource. The mean HEP for every DT path is calculated by fitting the distribution into a lognormal function.

AR: Key Alarm Not Attended To

DT path	PIFs (DT branch point)			1%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Distraction	HSI	Perceived Urgency						
1	High	Poor	Low	5.0E-02		2.0E-01		1.0E+00	2.5E-01
2	High	Poor	High	1.0E-03	1.0E-02	4.0E-02	1.0E-01	5.0E-01	9.8E-02
3	High	Good	Low	1.0E-03	1.0E-02	4.0E-02	5.0E-02	1.0E-01	6.5E-02
4	High	Good	High	5.0E-04	3.0E-04	3.0E-03	2.0E-02	3.0E-02	4.4E-03
5	Low	Poor	Low	1.0E-04	1.0E-03	3.0E-03	8.0E-03	5.0E-02	7.3E-03
6	Low	Poor	High	1.0E-05	1.0E-04	5.0E-04	8.0E-04	2.0E-03	9.6E-04
7	Low	Good		5.0E-07	1.0E-06	8.0E-06	1.0E-04	5.0E-04	2.4E-05

SA-1: Data Misleading or Not Available

DT path	PIFs (DT branch point)				1%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Alternate Source of Information	Information Obviously Incorrect	Guidance to Seek Confirmatory Data	Distraction						
1	No									
2	Yes	No	No	High	5.0E-02	8.0E-02	3.0E-01	5.0E-01	9.0E-01	3.6E-01
3	Yes	No	No	Low	1.0E-02	2.0E-02	2.0E-01	5.0E-01	9.0E-01	3.2E-01
4	Yes	No	Yes	High	5.0E-04	1.0E-03	5.0E-02	2.0E-01	5.0E-01	1.5E-01
5	Yes	No	Yes	Low	5.0E-04	1.0E-03	5.0E-03	1.0E-02	1.0E-01	9.6E-03
6	Yes	Yes	No	High	1.0E-02	2.0E-02	8.0E-02	4.0E-01	5.0E-01	1.1E-01
7	Yes	Yes	No	Low						1.2E-02
8	Yes	Yes	Yes	High	5.0E-03	1.0E-02	4.0E-02	2.0E-01	2.5E-01	3.1E-02
9	Yes	Yes	Yes	Low						3.4E-03

SA-2: Wrong Data Source Attended to

DT path	PIFs (DT branch point)				5%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	HSI	Workload	Familiarity with Data Source	Recovery						
1	Poor	High	Poor	No	1.0E-02		5.0E-02		5.0E-01	8.2E-02
2	Poor	High	Poor	Yes	5.0E-04		8.0E-03		5.0E-01	3.9E-02
3	Poor	High	Good	No	2.0E-03		2.0E-02		1.0E-01	2.5E-02
4	Poor	High	Good	Yes	3.3E-04		3.3E-03		1.7E-02	4.2E-03
5	Poor	Low	Poor	No	4.0E-03		2.0E-02		2.0E-01	3.3E-02
6	Poor	Low	Poor	Yes	6.7E-04		3.3E-03		3.3E-02	5.4E-03
7	Poor	Low	Good	No	1.0E-03		4.0E-03		5.0E-02	7.2E-03
8	Poor	Low	Good	Yes	1.7E-04		6.7E-04		8.3E-03	1.2E-03
9	Good	High	Poor	No	5.0E-04		3.0E-03		5.0E-02	6.2E-03
10	Good	High	Poor	Yes	8.3E-05		3.0E-04		8.3E-03	8.3E-04
11	Good	High	Good	No	2.4E-04		1.3E-03		1.2E-02	2.0E-03
12	Good	High	Good	Yes	3.9E-05		2.0E-04		2.0E-03	3.2E-04
13	Good	Low	Poor	No	2.4E-04		1.3E-03		1.2E-02	2.0E-03
14	Good	Low	Poor	Yes	3.9E-05		2.0E-04		2.0E-03	3.2E-04
15	Good	Low	Good	No	1.0E-05		2.0E-04		5.0E-03	5.2E-04
16	Good	Low	Good	Yes	1.0E-06		2.0E-05		5.0E-04	5.2E-05

SA-3: Critical Data Misperceived

DT path	PIFs (DT branch point)				1%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	HSI	Workload	Training	Recovery						
1	Poor	High	Poor	No	1.0E-01	2.0E-01	5.0E-01	8.0E-01	9.9E-01	5.6E-01
2	Poor	High	Poor	Yes		1.0E-02	5.0E-02	1.0E-01		5.7E-02
3	Poor	High	Good	No		7.0E-03	1.0E-02	4.0E-02		1.1E-02
4	Poor	High	Good	Yes		1.0E-04	3.0E-03	2.0E-02		5.7E-03
5	Poor	Low	Poor	No		1.0E-04	4.0E-03	1.0E-02		6.5E-03
6	Poor	Low	Poor	Yes		2.0E-05	8.0E-04	2.0E-03		1.3E-03
7	Poor	Low	Good	No		2.0E-06	8.0E-05	2.0E-04		1.3E-04
8	Poor	Low	Good	Yes		4.0E-07	1.6E-05	4.0E-05		2.6E-05
9	Good	High	Poor	No		1.0E-04	3.0E-03	2.0E-02		5.7E-03
10	Good	High	Poor	Yes		3.0E-05	1.0E-04	1.0E-03		1.3E-04
11	Good	High	Good	No		1.0E-05	1.0E-04	1.0E-03		1.6E-04
12	Good	High	Good	Yes		2.0E-05	3.0E-05	2.0E-04		3.4E-05
13	Good	Low	Poor	No		1.0E-05	8.0E-05	1.0E-03		1.3E-04
14	Good	Low	Poor	Yes		2.0E-06	1.0E-05	1.0E-04		1.3E-05
15	Good	Low	Good	No		3.0E-06	1.0E-05	1.0E-04		1.3E-05
16	Good	Low	Good	Yes		3.0E-06	1.0E-05	1.0E-04		1.3E-05

SA-4: Critical Data Dismissed/Discounted

DT path	PIFs (DT branch point)					1%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Valid Alternative DT path	Inappropriate Bias	Indications Reliable	Confirmatory Information	Recovery potential						
1	Yes	Formed	No	No	No	2.0E-03	2.0E-02	2.0E-01	5.0E-01	1.0E+00	4.9E-01
2	Yes	Formed	No	No	Yes		2.0E-03	2.0E-02	5.0E-02		5.0E-02
3	Yes	Formed	No	Yes	No		1.0E-04	4.0E-04	1.0E-03		4.5E-02
4	Yes	Formed	No	Yes	Yes		1.0E-03	4.0E-03	1.0E-02		4.5E-03
5	Yes	Formed	Yes	No	No		1.0E-02	1.0E-01	2.5E-01		2.5E-01
6	Yes	Formed	Yes	No	Yes		1.0E-03	1.0E-02	2.5E-02		2.5E-02
7	Yes	Formed	Yes	Yes	No		1.0E-03	1.0E-02	2.5E-02		2.5E-02
8	Yes	Formed	Yes	Yes	Yes		1.0E-04	1.0E-03	2.5E-03		2.5E-03
9	Yes	Not Formed	No	No	No		1.0E-04	2.0E-03	1.0E-02		3.3E-03
10	Yes	Not Formed	No	No	Yes		1.0E-05	2.0E-04	1.0E-03		3.3E-04
11	Yes	Not Formed	No	Yes	No		1.0E-05	2.0E-04	8.0E-04		3.1E-04
12	Yes	Not Formed	No	Yes	Yes		6.0E-04	3.0E-05	2.0E-04		3.1E-05
13	Yes	Not Formed	Yes	No	No		1.0E-04	1.0E-03	1.0E-02		1.6E-03
14	Yes	Not Formed	Yes	No	Yes		1.0E-05	1.0E-04	1.0E-03		1.6E-04
15	Yes	Not Formed	Yes	Yes			3.0E-06	1.0E-05	1.0E-04		1.3E-05
16	No										

SA-5: Premature Termination of Critical Data Collection

DT path	PIFs (DT branch point)					5%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Viable plant status believable	Expectations or Biases	Workload	HSI	Recovery potential						
1	Yes	Formed	High	Poor	No	1.0E-02		7.0E-02		7.0E-01	1.1E-01
2	Yes	Formed	High	Poor	Yes	5.0E-04		7.0E-03		1.0E-01	1.3E-02
3	Yes	Formed	High	Good	No	5.0E-03		4.0E-02		2.0E-01	5.1E-02
4	Yes	Formed	High	Good	Yes	5.0E-04		4.0E-03		2.0E-02	5.1E-03
5	Yes	Formed	Low	Poor	No	6.7E-03		4.6E-02		4.7E-01	7.6E-02
6	Yes	Formed	Low	Poor	Yes	6.7E-04		4.6E-03		4.7E-02	7.6E-03
7	Yes	Formed	Low	Good	No	4.0E-04		5.0E-03		5.0E-02	8.2E-03
8	Yes	Formed	Low	Good	Yes	4.0E-05		5.0E-04		5.0E-03	8.2E-04
9	Yes	Not Formed	High	Poor	No	1.3E-03		7.0E-03		9.3E-02	1.3E-02
10	Yes	Not Formed	High	Poor	Yes	1.3E-04		7.0E-04		9.3E-03	1.3E-03
11	Yes	Not Formed	High	Good	No	1.0E-04		1.0E-03		5.0E-02	4.1E-03
12	Yes	Not Formed	High	Good	Yes	1.0E-05		1.0E-04		5.0E-03	4.1E-04
13	Yes	Not Formed	Low	Poor	No	1.0E-04		3.0E-03		2.0E-02	4.2E-03
14	Yes	Not Formed	Low	Poor	Yes	1.0E-05		3.0E-04		2.0E-03	4.2E-04
15	Yes	Not Formed	Low	Good	No	1.0E-05		1.0E-04		4.0E-03	3.5E-04
16	Yes	Not Formed	Low	Good	Yes	1.0E-06		1.0E-05		4.0E-04	3.5E-05
17	No										

RP-1: Misinterpret Procedure

DT path	PIFs (DT branch point)				1%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Procedure Open to Misinterpretation	Workload	Training	Recovery						
1	Yes	High	Less than adequate	No	7.0E-02	1.0E-01	2.0E-01	5.0E-01	8.0E-01	2.3E-01
2	Yes	High	Less than adequate	Yes	2.0E-03	4.0E-03	2.0E-02	1.0E-01	2.0E-01	3.3E-02
3	Yes	High	Good	No	1.0E-03	5.0E-03	3.0E-02	5.0E-02	5.0E-01	7.3E-02
4	Yes	High	Good	Yes	2.0E-05	5.0E-04	1.0E-03	5.0E-03	1.0E-01	5.3E-03
5	Yes	Low	Less than adequate	No	1.0E-03	5.0E-03	3.0E-02	2.0E-01	5.0E-01	7.3E-02
6	Yes	Low	Less than adequate	Yes	2.0E-04	7.0E-04	2.0E-03	5.0E-03	3.0E-02	3.6E-03
7	Yes	Low	Good		1.0E-05	3.0E-05	1.0E-04	3.0E-04	1.0E-03	1.6E-04
8	No									

RP-2: Choose Inappropriate Strategy

DT path	PIFs (DT branch point)			5%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Preference for correct strategy	Advantage to the correct strategy	Recovery potential						
1	Low	No	No	6.0E-02		5.0E-01		9.0E-01	5.2E-01
2	Low	No	Yes	5.0E-03		5.0E-02		5.0E-01	8.2E-02
3	Low	Yes	No	5.0E-03		1.0E-01		7.0E-01	1.4E-01
4	Low	Yes	Yes	5.0E-04		1.0E-02		7.0E-02	1.4E-02
5	High	No	No	2.0E-03		2.0E-02		2.0E-01	3.3E-02
6	High	No	Yes	2.0E-04		2.0E-03		2.0E-02	3.3E-03
7	High	Yes	No	1.0E-05		3.0E-03		1.0E-01	9.3E-03
8	High	Yes	Yes	1.0E-06		3.0E-04		1.0E-02	9.3E-04

E-1: Delay Implementation

DT path	PIFs (DT branch point)			1%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Reluctance & Viable Alternative	Assessment of Margin	Additional Cues						
1	Exists	Incorrect	No	1.0E-03	1.0E-02	7.0E-02	4.0E-01	5.0E-01	1.7E-01
2	Exists	Incorrect	Yes	5.0E-04	5.0E-03	1.0E-02	5.0E-02	2.0E-01	1.1E-02
3	Exists	Correct	No	5.0E-04	2.0E-03	2.0E-02	5.0E-02	1.0E-01	3.8E-02
4	Exists	Correct	Yes	1.0E-04	1.0E-03	5.0E-03	3.0E-02	1.0E-01	6.5E-03
5	Absent	Incorrect	No	2.0E-06	2.0E-05	1.4E-04	8.0E-04	1.0E-03	3.4E-03
6	Absent	Incorrect	Yes	6.7E-05	6.7E-04	4.7E-03	2.7E-02	3.3E-02	2.2E-04
7	Absent	Correct							1.7E-05

E-2: Critical Data Not Checked with Appropriate Frequency

DT path	PIFs (DT branch point)				5%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Monitoring Optimized	Importance of Data Understood	Match with Expectations	Alarm						
1	No	No	Poor	No	1.0E-01		4.0E-01		9.0E-01	4.3E-01
2	No	No	Poor	Yes	2.2E-03		1.0E-02		2.0E-02	1.0E-02
3	No	No	Good	No	7.7E-03		3.0E-02		6.9E-02	3.2E-02
4	No	No	Good	Yes	7.0E-04		7.0E-03		3.0E-02	8.5E-03
5	No	Yes	Poor	No	3.3E-03		1.3E-02		3.0E-02	1.4E-02
6	No	Yes	Poor	Yes	7.4E-05		3.0E-04		6.7E-04	3.2E-04
7	No	Yes	Good	No	0.001?		1.0E-02		5.0E-02	1.3E-02
8	No	Yes	Good	Yes	5.7E-06		1.0E-03		5.1E-05	2.3E-03
9	Yes		Poor	No	1.4E-03		1.1E-02		4.5E-02	1.3E-02
10	Yes		Poor	Yes	3.0E-05		2.0E-04		1.0E-03	2.5E-04
11	Yes		Good	No	4.5E-04		1.5E-03		1.4E-02	2.3E-03
12	Yes		Good	Yes	1.0E-05		3.0E-05		3.0E-04	4.9E-05

E-3: Failure to Initiate Execution

DT path	PIFs (DT branch point)			5%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Immediacy	Workload	Recovery potential						
1	No	High	No	1.0E-02		1.0E-01		8.0E-01	1.5E-01
2	No	High	Yes	3.0E-03		1.0E-02		1.0E-01	1.6E-02
3	No	Low	No	1.0E-03		5.0E-03		5.0E-02	8.2E-03
4	No	Low	Yes	1.0E-04		5.0E-04		5.0E-03	8.2E-04
5	Yes			1.0E-05		8.0E-05		1.0E-03	1.4E-04

E-4: Failure to Correctly Execute Response (Simple Task)

DT path	PIFs (DT branch point)			1%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	HSI	Workload	Recovery						
1	Poor	High	No	1.0E-03	2.0E-03	2.0E-02	5.0E-02	1.0E-01	3.3E-02
2	Poor	High	Yes	2.0E-04	4.0E-04	4.0E-03	1.0E-02	2.0E-02	6.6E-03
3	Poor	Low	No	1.0E-03	2.0E-03	2.0E-02	5.0E-02	1.0E-01	3.3E-02
4	Poor	Low	Yes	2.0E-04	4.0E-04	4.0E-03	1.0E-02	2.0E-02	6.6E-03
5	Nominal	High	No			3.0E-06	3.0E-05	1.0E-04	9.3E-06
6	Nominal	High	Yes			1.0E-06	1.0E-05		1.6E-06
7	Nominal	Low	No			3.0E-06	3.0E-05	1.0E-04	9.3E-06
8	Nominal	Low	Yes			1.0E-06	1.0E-05		1.6E-06

E-5: Failure to Correctly Execute Response (Complex Task)

DT path	PIFs (DT branch point)				1%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Execution straightforward	Training	Work practice	Recovery						
1	No	Poor	Poor	No	5.0E-02	6.0E-02	9.0E-02	3.0E-01	5.0E-01	E-1
2	No	Poor	Poor	Yes	1.0E-03	3.0E-03	1.0E-02	3.0E-02	1.0E-01	1.6E-02
3	No	Poor	Good	No	5.0E-04	4.0E-03	2.0E-02	1.0E-01	3.0E-01	5.1E-02
4	No	Poor	Good	Yes	5.0E-05	4.0E-04	2.0E-03	1.0E-02	3.0E-02	5.1E-03
5	No	Good	Poor	No	1.0E-04	1.0E-03	5.0E-03	1.0E-01	2.0E-02	9.6E-03
6	No	Good	Poor	Yes	1.0E-05	1.0E-04	5.0E-04	1.0E-02	2.0E-03	9.6E-04
7	No	Good	Good	No	5.0E-05	5.0E-04	2.0E-03	5.0E-03	1.0E-02	3.8E-03
8	No	Good	Good	Yes	5.0E-06	5.0E-05	2.0E-04	5.0E-04	1.0E-03	3.8E-04
9	Yes	Poor	Poor	No	5.0E-04	8.0E-03	5.0E-03	1.0E-02	1.0E-01	9.6E-03
10	Yes	Poor	Poor	Yes	1.0E-05	2.0E-05	8.0E-05	3.0E-04	1.0E-03	1.3E-04
11	Yes	Poor	Good	No	1.0E-05	5.0E-05	4.0E-04	8.0E-04	5.0E-03	9.8E-04
12	Yes	Poor	Good	Yes	5.0E-06	7.0E-06	3.0E-05	7.0E-05	1.0E-03	5.7E-05
13	Yes	Good	Poor	No	4.0E-05	6.4E-04	4.0E-04	8.0E-04	8.0E-03	8.0E-04
14	Yes	Good	Poor	Yes						8.0E-05
15	Yes	Good	Good	No	8.0E-07	4.0E-06	3.2E-05	6.4E-05	4.0E-04	8.0E-05
16	Yes	Good	Good	Yes	1.0E-07	5.0E-07	4.0E-06	8.0E-06	5.0E-05	E-5

AP-1 Misread or Skip Step in Procedure

DT path	PIFs (DT branch point)				5%-tile	10%-tile	50%-tile	90%-tile	99%-tile	Mean
	Workload	Procedure	Compensatory factors	Recovery potential						
1	High	Complex	Not present	No	1.0E-02		8.0E-02		3.0E-01	9.4E-02
2	High	Complex	Not present	Yes	1.4E-03		1.1E-02		4.3E-02	1.3E-02
3	High	Complex	Present	No	2.0E-03		1.6E-02		6.0E-02	1.9E-02
4	High	Complex	Present	Yes	2.9E-04		2.3E-03		8.6E-03	2.7E-03
5	High	Simple	Not present	No	1.4E-03		1.1E-02		4.3E-02	1.3E-02
6	High	Simple	Not present	Yes	2.0E-04		1.6E-03		6.1E-03	1.9E-03
7	High	Simple	Present	No	7.0E-05		6.0E-04		7.0E-03	1.0E-03
8	High	Simple	Present	Yes	1.0E-05		8.6E-05		1.0E-03	1.5E-04
9	Low	Complex	Not present	No	1.8E-03		3.5E-02		5.5E-02	3.6E-02
10	Low	Complex	Not present	Yes	2.6E-04		5.0E-03		7.8E-03	5.1E-03
11	Low	Complex	Present	No	7.0E-05		7.0E-04		1.0E-02	1.3E-03
12	Low	Complex	Present	Yes	1.0E-05		E-5		1.4E-03	9.7E-05
13	Low	Simple		No	2.0E-05		5.0E-04		5.0E-03	8.2E-04
14	Low	Simple		Yes	7.0E-06		7.0E-05		8.0E-04	1.2E-04