NUREG-2199, Vol. 3

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Testing the Integrated Human Event Analysis System for Nuclear Power Plant Internal Events At-Power Application (IDHEAS AT-POWER)

Volume 3

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at the NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Mail Stop SSOP
   Washington, DC 20402-0001
   Internet: http://bookstore.gpo.gov
   Telephone: 1-866-512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Road
   Alexandria, VA 22161-0002
   http://www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

U.S. Nuclear Regulatory Commission
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at the NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
http://www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG-XXXX) or agency contractors (NUREG/CR-XXXX), (2) proceedings of conferences (NUREG/CP-XXXX), (3) reports resulting from international agreements (NUREG/IA-XXXX), (4) brochures (NUREG/BR-XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG-0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Testing the Integrated Human Event Analysis System for Nuclear Power Plant Internal Events At-Power Application (IDHEAS AT-POWER)

Volume 3

Manuscript Completed: ~~May 2017~~
Date Published: ~~May~~ ~~2022~~

Prepared by:
H. Liao[1]
S. Morrow[2]
G. Parry[3]
M. Presley[4]
L. Criscione[2]
D. Bley[5]

[1]Sandia National Laboratory
[2]U.S. Nuclear Regulatory Commission
[3]Jensen Hughes, Inc.
[4]Electric Power Research Institute
[5]The WreathWood Group

Stephanie Morrow, NRC Project Manager

Office of Nuclear Regulatory Research

ABSTRACT

This report documents a study of the Integrated Human Event Analysis System for nuclear power plant internal events at-power application (IDHEAS AT-POWER), a human reliability analysis method developed by the U.S. Nuclear Regulatory Commission and the Electric Power Research Institute. The purpose of the study was to perform a holistic test of the method to identify strengths and weaknesses. Five analyst teams applied the method to analyze five predefined human failure events for three scenarios in a pressurized water reactor. The study evaluated the method against five criteria: validity, inter-analyst consistency, traceability, usability, and utility. The results indicated that IDHEAS AT-POWER provides a structured analysis framework and traceable quantification approach to HRA. However, there was variability in the results between analyst teams, particularly in the assessment of execution tasks and credit for recovery. The report presents a discussion of the strengths and weaknesses of IDHEAS AT-POWER, lessons learned from the study, recommendations for improvement in the method guidance, and suggestions for future method development.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

This report documents a study of the Integrated Human Event Analysis System for nuclear power plant internal events at-power application (IDHEAS AT-POWER). IDHEAS AT-POWER is a human reliability analysis (HRA) method developed by the U.S. Nuclear Regulatory Commission in collaboration with the Electric Power Research Institute. The purpose of the study was to perform a holistic test of the IDHEAS AT-POWER method to identify strengths and weaknesses and determine whether diverse teams can practically apply the method to produce consistent HRA results.

Methodology

Five HRA analyst teams applied the IDHEAS AT-POWER method to analyze five human failure events (HFEs), predefined for three scenarios in a pressurized water reactor.

- Scenario 1 described a standard steam generator tube rupture (SGTR). The HFE associated with Scenario 1 was defined as failure to isolate the ruptured steam generator and control pressure below the steam generator Pressure Operated Relief Valve (PORV) setpoint before steam generator PORV opening (HFE 1).
- Scenario 2 described a total loss of feedwater with a misleading indicator of flow to the steam generators. The HFE associated with Scenario 2 was defined as failure to establish bleed and feed within 45 minutes of the reactor trip, given that the crews initiate a manual reactor trip before an automatic reactor trip (HFE 2).
- Scenario 3 was adapted from an actual event in a nuclear power plant and described an electrical fire that caused a reactor trip and subsequent loss of reactor coolant pump (RCP) seal injection and cooling. There were three HFEs associated with Scenario 3.
    - Failure to restore component cooling water to the reactor coolant pump thermal barrier heat exchangers by reopening FCV-626 (HFE 3).
    - Failure to trip the reactor coolant pumps during a loss of all seal cooling and injection (HFE 4).
    - Failure to depressurize the reactor coolant system during a small loss-of-coolant accident (HFE 5).

Evaluation Criteria

The study evaluated the IDHEAS AT-POWER method against five criteria:

- **Validity:** Whether the method provides a reasonable assessment of human reliability.
- **Inter-analyst consistency:** The extent to which different HRA analyst teams produced the same or similar results when using the IDHEAS AT-POWER guidance.
- **Traceability:** The extent to which IDHEAS AT-POWER documentation provided a clear link from the qualitative analysis to the quantitative inputs, and then to the human error probabilities.
- **Usability:** The quality of the analysts' experience with using the method for HRA.

- **Utility:** The extent to which the method provided useful information for decisionmaking, including its ability to identify potential error reduction measures.

Results and Discussion

By allowing analysts to go through the entire HRA process, the holistic test of IDHEAS AT-POWER indicated where variability can occur in the analysis and identified potential gaps and areas for improvement.

The results of the study indicated that IDHEAS AT--POWER provides a structured analysis framework and highly traceable quantification approach to HRA. The structured qualitative analysis framework encouraged a detailed assessment of timelines, procedures, and plant conditions. The traceability enabled identification of sources of inter-analyst variability, assessment of whether the rationale underlying the analysis was reasonable, and evaluation of the impact of the assumptions made in the analysis. The traceability of the analysis process can lead to a more defensible basis for assessing scenario-specific performance issues and influencing factors. The documentation also enabled a third-party review to identify sources of inter-analyst variability, assess whether the rationale underlying the analysis was reasonable, and evaluate the impact of the assumptions made in the analysis. Moreover, the level of detail in the analysis increased the utility of the method by identifying areas for operator performance improvement.

Not surprisingly considering the uncertainties in HRA and the results of past benchmark studies, the study found variability in the results between analyst teams, particularly in the assessment of execution tasks and credit for recovery. Conversely, there were also multiple examples of inter-analyst consistency. This points to evidence that IDHEAS AT-POWER provides an analysis framework that can enhance inter-analyst consistency, but some methodological and guidance limitations can make it difficult to achieve inter-analyst consistency throughout the analysis process.

The study also found that the detailed analysis process can be resource intensive. The analysts reported a significant learning curve when it came to assessing crew failure modes and performance influencing factors. The detailed analysis of procedural steps and assessment of the scenario context required significant operations knowledge. This highlights the importance of adequate training and practice for analysts to efficiently apply the method, and operations input to appropriately apply the method. It should be recognized that the benefits of the detailed analysis may outweigh the additional resource costs for complex, cognitively demanding scenarios where traceability and utility are critically important. Moreover, the resource requirements can likely be reduced with a computerized tool and elimination of redundant documentation.

Recommendations

Based on the findings from the study, a number of recommendations are included in the report with respect to training, method guidance improvement, and future method development.

Training and guidance may be improved by focusing on (1) aspects that are unique to IDHEAS AT-POWER or similar but different from other HRA methods, and (2) method nuances or circumstances where extra caution is needed in method implementation. Furthermore, time and practice are needed for analysts to fully understand the method guidance. Particular areas of focus for enhanced training and guidance may include:

- Construction of the crew response diagram and task decomposition
- Guidance for holistic categorization of execution actions
- Assessment of crew failure modes and performance influencing factors
- Recovery modeling

Recommendations that are beyond the scope of the current method, but should be considered for future method development include:

- Inclusion of additional crew failure modes
- Further evaluation and calibration of failure probabilities based on human performance data
- Evaluation of the additive effects of small human error probabilities
- Computerization of the IDHEAS AT-POWER method
- Evaluation of suitability of holistic treatment of execution actions
- Evaluation of approach to addressing uncertainty in procedural paths

ACKNOWLEDGEMENTS

The authors would like to thank the analysts who participated in the testing: David Aird, Jerrod Demers, Michelle Kichline, Kendra Wright, Dale Yielding, Lynn Kolonauski, Don MacLeod, Vicki Manning, Robert Lichtenstein, and Eric Jorgenson. Their engagement in the testing process and their feedback provided invaluable insights into the practical use of the IDHEAS AT-POWER human reliability analysis method. Special thanks also to Stacey Hendrickson at Sandia National Laboratories for her assistance with training analysts on using the IDHEAS AT-POWER method, and Jing Xing at the U.S. Nuclear Regulatory Commission for her guidance in developing the project plan, training materials, and testing protocol.

ABBREVIATIONS AND ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
AFW	auxiliary feedwater
AOP	abnormal operating procedure
ASP	Accident Sequence Precursor
ATHEANA	A Technique for Human Event ANAlysis
B&F	bleed and feed
BOP	balance of plant
BWR	boiling water reactors
CCW	component cooling water
CD	core damage
CFM	crew failure mode
CRD	crew response diagram
CSF	critical safety functions
CVC	chemical and volume control
EDG	emergency diesel generators
EOL	end of life
EOP	emergency operating procedure
EPP	end path procedure
EPRI	Electric Power Research Institute
FCV	flow control valve
HEP	human error probability
HFE	human failure event
HRA	human reliability analysis
HSI	human system interface
IDHEAS	IntegrateD Human Event Analysis System
LOCA	loss of coolant accident
LOFW	loss of feedwater
LOSC	loss of seal cooling
MFW	main feedwater
MSIV	main steam isolation valves
MSR	moisture separator reheater
NPP	nuclear power plant
NR	narrow range
NRC	U.S. Nuclear Regulatory Commission
PIF	performance-influencing factor
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PSF	performance shaping factor

PWR	pressurized water reactor
RCP	reactor coolant pump
RCS	reactor coolant system
RHR	residual heat removal
RO	reactor operator
RPD	recognition primed decision
RWST	refueling water storage tank
SDC	shutdown cooling
SDP	Significance Determination Process
SG	steam generator
SGTR	steam generator tube rupture
SI	safety injection
SLOCA	small loss-of-coolant accident
SME	subject matter expert
SPAR-H	Standardized Plant Analysis Risk - Human reliability analysis
SRM	staff requirements memorandum
SRO	senior reactor operator
STA	shift technical advisor
THERP	Technique for Human Error Rate Prediction
VCT	volume control tank

1 INTRODUCTION

1.1 Background

Human reliability analysis (HRA) uses systems engineering and behavioral science methods to assess the human contribution to risk and to identify ways to reduce that risk. It is used in the context of probabilistic risk assessment (PRA) to provide risk information regarding human performance to support risk-informed decisionmaking with respect to high-reliability industries. For example, the U.S. Nuclear Regulatory Commission (NRC) considers risk information from HRAs an important input to licensing and regulatory decisions.

Variability in HRA results among different HRA analysts is still a significant issue, even when analysts are using state-of-the-art methodologies. The variability in HRA results in turn contributes to uncertainty in PRA results. There are several sources of variability, which are most commonly attributed to the existence and use of different HRA methods that rely on different assumptions, human performance frameworks, and quantification algorithms. However, another source of variability is inconsistent implementation, even when analysts use the same methods. This results in concerns over the robustness of HRA methods.

1.2 IDHEAS-AT POWER Method

The Integrated Human Event Analysis System for nuclear power plant internal events at-power application (hereafter "IDHEAS AT-POWER") [1] was developed as a joint effort between the U.S. NRC and Electric Power Research Institute (EPRI). Some of the objectives were to develop an HRA method that enhances the use of qualitative analysis, reduces analyst-to-analyst variability, provides traceable and reproducible results, and improves estimates of human error probabilities (HEPs). The IDHEAS AT-POWER method includes the following key elements (see the full report [1] for more information on the method).

1. Description of the accident scenario and analysis of the human performance challenges in the scenario.
2. Identification and definition of human failure events (HFEs) that represent those failures that have an impact on the outcome of the scenarios.
3. Feasibility analysis of the required responses including consideration of time constraints.
4. Task analysis and development of a crew response diagram (CRD). The crew response diagram is a graphical representation that identifies the expected crew response paths, the critical tasks required for successful response, and recovery (correction) potential for errors in performing those critical tasks. It supports documentation of the qualitative analysis.
5. Implementation of the method's quantification model to estimate the human error probabilities. The quantification model provides a set of 14 crew failure modes (CFMs), a decision tree for each crew failure mode that includes the most relevant performance-influencing factors (PIFs), and expert-estimated human error probabilities of every crew failure mode under different combinations of the performance-influencing factors.
6. Model integration by analyzing dependencies between the human failure events in a PRA sequence, identifying and analyzing recovery actions, and documenting uncertainties in the HRA.

1.3 Purpose of Study

The purpose of the present study was to test IDHEAS AT-POWER and evaluate whether diverse teams can practically apply the method to produce consistent HRA results. It should be noted that due to constraints on the scope, the study did not test some features of the method (e.g., time uncertainty analysis and dependency analysis). In addition, the study predefined the event tree representations and human failure events for the accident scenarios.

2 STUDY METHODOLOGY

To achieve the goal of evaluating whether IDHEAS AT-POWER can be practically applied to produce consistent HRA results, the study sought to perform a more holistic test of the method, rather than a narrowly focused test on certain elements of the method. The study undertook this holistic approach to approximate the reality of how an HRA is performed. The holistic approach provided analysts with an opportunity to go through the whole HRA process, and thus allowed the study to identify steps in the process that were particularly vulnerable to variability in the HRA estimates. Previous studies have demonstrated that many factors may cause variability in HRA estimates [2].

Any test of an HRA method will encounter challenges in experimental design and control [5]. Ideally, sufficient human performance data is needed to evaluate whether the method estimates are reasonable assessments of human reliability. Furthermore, an ideal test requires a range of tasks, scenarios, and HRA analyst teams, so that sufficient data can be generated to establish conclusive findings. However, the ideal is not practical given the limited availability of empirical data, the current state-of-the-art of HRA, and other constraints on time and resources. Hence, a balance between the ideal and the practical is needed in the design, planning, and execution of the study. In addition, since an important aspect of the study is to understand why different results are obtained across HRA analyst teams, it is important to provide adequate controls that allow direct team-to-team comparison and inferences about the causes of variation in results.

The following sections describe the study methodology. The methodology included certain trade-offs to constrain the study design to one that was practical to implement while also minimizing undesired effects and potential confounding influences.

2.1 Testing Scenarios and Human Failure Events

Ideally, a range of scenarios and tasks should be considered to have a complete representation of the capabilities of IDHEAS AT-POWER. These scenarios and tasks should also be representative of those that could occur in the nuclear power industry (i.e., the types of tasks that would be analyzed in real risk assessment). The study used three pressurized-water reactor (PWR) scenarios for testing. The first two scenarios were adapted from NUREG-2156, "The U.S. HRA Empirical Study - Assessment of HRA Method Predictions against Operating Crew Performance on a U.S. Nuclear Power Plant Simulator," hereafter referred to as the U.S. HRA Empirical Study [2], with one human failure event (HFE) predefined for each. Scenario 1 described a standard steam generator tube rupture (SGTR), and Scenario 2 described a total loss of feedwater with a misleading indicator of flow to the steam generators. The study adapted Scenario 3 from an actual event in a nuclear power plant, for which three human failure events were defined. Scenario 3 described an electrical fire that caused a reactor trip and subsequent loss of reactor coolant pump (RCP) seal injection and cooling.

Some considerations were taken in selecting the scenarios to minimize the impact of the small number of scenarios and human failure events. First, the scenarios should vary in complexity and encompass a broad spectrum of activities encountered in HRA such that the strengths and weaknesses of IDHEAS AT-POWER can be effectively assessed. For example, Scenario 1 was selected to represent a very straightforward scenario, whereas Scenario 2 was selected to represent a more cognitively complicated scenario. This allows for an evaluation of whether analysts' estimates using IDHEAS AT-POWER are sensitive to scenario differences and whether the estimates are adjusted accordingly. Given the small number of scenarios,

complicated scenarios and human failure events are important in that they can simulate a broad range of performance issues to test an HRA method's capabilities to identify them.

Second, the human failure events defined in the study should be plausible. The human failure event definitions for Scenario 1 and 2 were based on those of similar human failure events from real plant PRAs. The human failure events in Scenario 3 were based on an actual event in a nuclear power plant, with some scenario detail deleted or summarized at a high level to allow analysts to (1) focus on the important aspects or effects of the scenario that led to the events requiring operator action, and (2) understand the event sequence and associated contextual factors. As a result, Scenario 1 and 2 were used to represent typical PRA applications, whereas Scenario 3 was included to represent real-world event analysis applications, such as the Accident Sequence Precursor (ASP) program and Significance Determination Process (SDP) at the NRC.

Third, the scenarios should leverage existing data and information from other tests of HRA methods. Scenarios 1 and 2 were simulated on a nuclear power plant simulator and analyzed with other HRA methods as part of the U.S. HRA Empirical Study [2].[1] The extent to which the IDHEAS AT-POWER estimates are comparable to the simulator data and other methods' estimates can provide additional evidence to support our assessment of the IDHEAS AT-POWER method's capabilities (see discussion in Section 3.1.2).

The scenarios and human failure events are briefly described in the following subsections. More detailed information is presented in Appendix A.2.

2.1.1 Scenario 1: Steam Generator Tube Rupture (SGTR)

Plant technical information

- 4-loop Westinghouse pressurized-water reactor (PWR)
- All participating crew members in control room (shift manager, unit supervisor, shift technical advisor and two reactor operators)
- The plant is operating at 100 percent

While operating at power, a tube rupture occurs in a steam generator. The leak size is about 500 GPM at 100 percent power, which is sufficient to cause nearly immediate secondary radiation alarms and other abnormal indications/alarms. The operators have about 3 hours to isolate the ruptured steam generator and maintain reactor coolant system pressure below the steam generator power-operated relief valve (PORV) setpoint by cooling down the reactor coolant system (RCS).

[1] Scenario 1 and HFE 1 in the IDHEAS AT-POWER test was the same as Scenario 3 and HFE 3A in the U.S. HRA Empirical Study. Scenario 2 and HFE 2 in the IDHEAS AT-POWER test was the same as Scenario 1 and HFE 1A in the U.S. HRA Empirical Study. Note that additional scenarios and HFEs were included in the U.S. HRA Empirical Study but were omitted from the test of IDHEAS AT-POWER.

The operator actions include:

- Isolate the ruptured steam generator (feedwater and main steam isolation valves closed).

- Maintain reactor coolant system pressure below the steam generator power-operated relief valve setpoint by cooling down the reactor coolant system (cooling the secondary by dumping steam and depressurizing the reactor coolant system).

Definition of Human Failure Event 1

Failure to isolate the ruptured steam generator and control pressure below the steam generator PORV setpoint before steam generator PORV opening. The time window to perform the required actions is estimated to be 3 hours.

2.1.2 Scenario 2: Total Loss of Feedwater (LOFW)

Plant technical information

- 4-loop Westinghouse pressurized-water reactor (PWR)

- There are three main feedwater (MFW) pumps, four auxiliary feedwater (AFW) pumps, and one start-up feed pump. Of the four AFW pumps, one is turbine driven and the other three motor driven.

- The shift technical advisor (STA) 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 (shift manager, unit supervisor, 2 reactor operators)

- The plant is operating at 100 percent

The plant is initially operating at 100 percent power when all main feedwater pumps are either lost or trip and the start-up feed pump cannot start. Three of the four auxiliary feedwater pumps fail after automatic start. The fourth auxiliary feedwater pump starts automatically and indicates full flow, but this flow will not reach the steam generators because a manual recirculation valve is mispositioned open. There is no indication of the valve's position in the control room. The steam generator levels will go down rapidly before the reactor is tripped. The plant computer will not show a red path on the heatsink status tree because of the indicated flow from the running auxiliary feedwater pump.

The crew will have to identify that the indicated auxiliary feedwater flow from the running auxiliary feedwater pump is not reaching any steam generator and enter the response to loss of secondary heat sink procedure (FRH1) to establish bleed and feed (B&F). All attempts to establish auxiliary feedwater before bleed and feed initiation will be forced to fail in the simulator.

Assuming the crew manually trips the reactor within approximately 30–to-45 seconds of the loss of feedwater, they will have approximately 45 minutes to initiate bleed and feed before core damage (CD).

The operator actions to start bleed and feed include:

- actuate safety injection
- open both of the pressurizer power-operated relief valves

Definition of Human Failure Event 2

Failure to establish bleed and feed within 45 minutes of the reactor trip, given that the crews initiate a manual reactor trip before an automatic reactor trip.

2.1.3 Scenario 3: Electrical Fault Causes Fire and Subsequent Reactor Trip with Loss of Reactor Coolant Pump (RCP) Seal Injection and Cooling

Plant technical information

- 3-loop Westinghouse pressurized-water reactor (PWR)
- There are two main feedwater (MFW) pumps, both of which are running.
- There are three charging pumps, two of which are running.
- There are three component cooling water (CCW) pumps, one of which is running.
- The plant is operating in Mode 1 at approximately 100 percent power.
- The shift manager and shift technical advisor are outside of the control room at a shift turnover meeting.

While operating at power, an electrical feeder cable failure caused a fire. The cable failure caused one reactor coolant pump (RCP) to trip, which in turn caused an automatic reactor trip, an automatic safety injection (SI), and other equipment malfunctions. Within the first minute of the initiating event, reactor coolant pump seal cooling is challenged when thermal barrier cooling is lost due to the closing of flow control valve (FCV) 626, a component cooling water thermal barrier outlet isolation valve. Approximately 27 minutes into the event, the charging flow is diverted from the reactor coolant pump seals to the reactor coolant system and reactor coolant pump seal injection becomes inadequate (there is some injection flow, but it is inadequate to fulfill its safety function) because chemical and volume control (CVC) valve 310A fails open. As a result, the reactor coolant pump seals begin to heat up and purge volume begins to empty.

For successful recovery, operators need to reopen FCV-626 from the control room within approximately 19 minutes after all reactor coolant pump seal cooling and injection are lost.

Definition of Human Failure Event 3

Failure to restore component cooling water to the reactor coolant pump thermal barrier heat exchangers by reopening FCV-626.

If FCV-626 is not opened in time or cannot be opened, operators have approximately 19 minutes from when seal cooling and injection are lost to trip the running reactor coolant pumps and avoid catastrophic seal failure.

Definition of Human Failure Event 4

Failure to trip the reactor coolant pumps during a loss of all seal cooling and injection.

If operators fail to stop the reactor coolant pumps, the reactor coolant pump seals will fail at the maximum leakage rate of 480 gpm per reactor coolant pump. The reactor coolant pump seal failure will lead to a small loss-of-coolant accident (SLOCA). The operators have at least two hours to initiate a cooldown and depressurization of the reactor coolant system prior to depletion of the refueling water storage tank inventory to allow for the plant to be placed in shutdown cooling (SDC) using the residual heat removal (RHR) system.

Definition of Human Failure Event 5

Failure to depressurize the reactor coolant system during a small loss-of-coolant accident.

2.2 Analyst Teams

One important aspect of the study design and control is the selection of HRA analyst teams. As mentioned earlier in this chapter, a sufficient number of analyst teams are needed to (1) control for potential team effects on the HRA results and (2) generate sufficient data from the test to increase confidence in the assessment findings. The study recruited four analyst teams: two from industry and two from the NRC. Each team consisted of two or three analysts. Although four is not a large number of teams, it was deemed sufficient to provide a range of data for the method testing. NUREG-2156, "The U.S. HRA Empirical Study," only used two analyst teams for most of the HRA methods tested and still identified many important strengths and weaknesses of the methods. The four teams selected provided a good representation of potential users of the method with analysts from both industry and the regulatory agency. An effort was made to control for levels of expertise and background across the teams to minimize the potential for team differences to affect the results.

Although each HRA team had combined familiarity with nuclear power plant engineering, operations, probabilistic risk assessment (PRA), and HRA, there were some apparent variations in expertise and knowledge in some areas across the teams. For instance, the NRC teams had significantly less overall experience with PRA than the industry teams. Additionally, although all teams had experience with nuclear power plant operations, one team's experience was primarily with boiling-water reactors (BWRs), which made it more challenging for that team to interpret the pressurized-water reactor scenarios and procedures used in the testing.

To control for potential bias from prior knowledge of the testing scenarios or the IDHEAS AT-POWER method, the analysts were screened to ensure that they had not been involved in past HRA method testing studies that used the same scenarios (e.g., NUREG-2156, "The U.S. HRA Empirical Study") or in the development of IDHEAS AT-POWER.

In addition, the project team (the authors of this report) also analyzed the scenarios with IDHEAS AT-POWER. They were treated as a fifth team (labeled as "Team 5" throughout the report) and their analyses were compared with those of the other teams.

2.3 Training

Before the HRA analyst teams used IDHEAS AT-POWER for testing, all teams were trained in a 2-day workshop to ensure that they fully understood the method and could use it independently. The project team, which included some of the method developers, developed the training materials and gave the lectures with examples and exercises.

The testing study occurred while the IDHEAS AT-POWER report was still undergoing revision. As a result, some of the training materials used for testing may differ from the final version of the method guidance.

Figure 2-1 shows an overview of the IDHEAS-AT POWER method as it was presented to the analyst teams as part of the training workshop. The training was structured using the six steps outlined on the left side of the overview graphic.

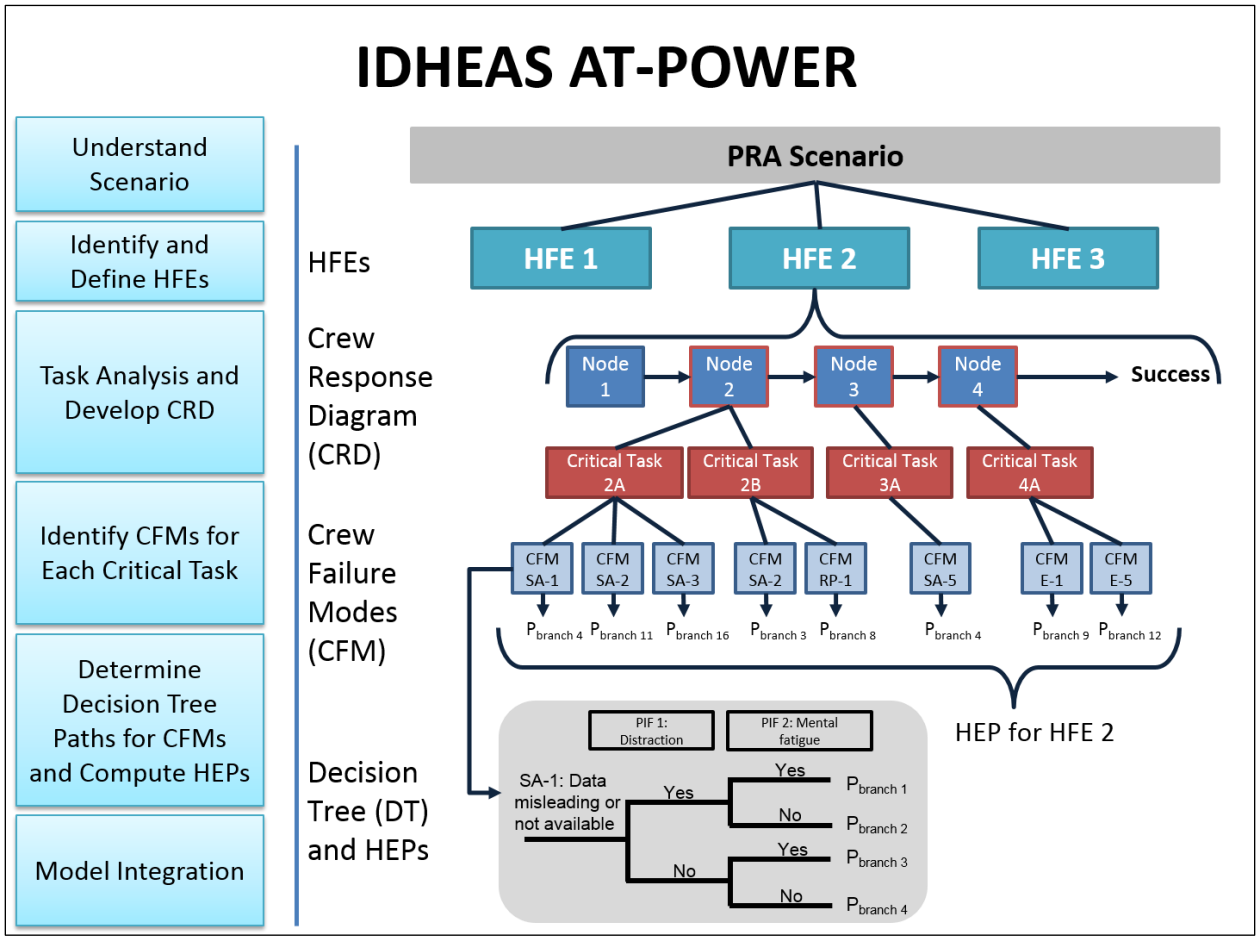


Figure 2-1 Overview of IDHEAS AT-POWER

Some of the more unique characteristics of IDHEAS AT-POWER are its use of a crew response diagram to graphically represent a crew's success path, and the selection of crew failure modes for each critical task identified in the task analysis. Figure 2-2~~Figure 2-2~~ displays a sample crew response diagram, which is the crew response diagram for the project team's analysis of

Human Failure Event 1. The numbered boxes on the crew response diagram are referred to as nodes. Each node represents major transition or decision points in the crew's response on the success path. Each crew response diagram node in blue represents one or more critical tasks that the crew must complete. The white nodes are included on the crew response diagram for informational purposes, and the green nodes represent potential recoveries. During the training, the analysts were advised that critical tasks are those tasks for which failure of the task would result in the human failure event. The analysts were instructed to assess each critical task and determine which crew failure modes would potentially apply to each critical task.

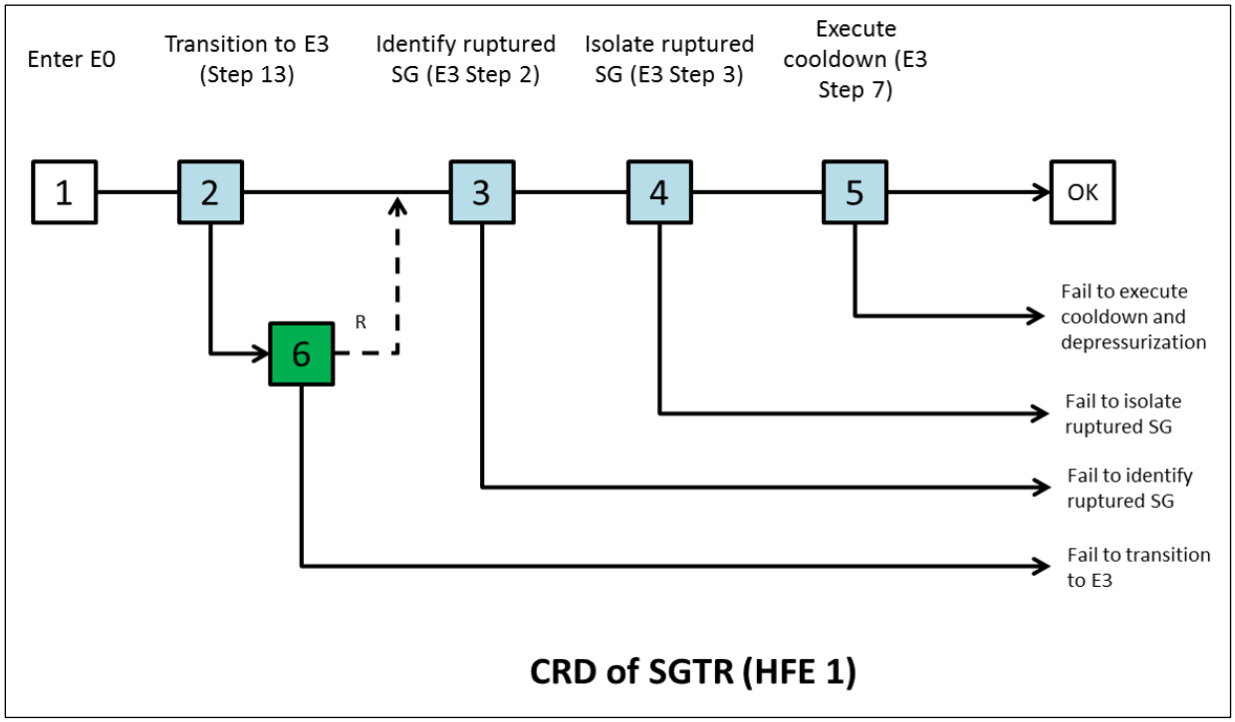


Figure 2-2 Sample Crew Response Diagram (Human Failure Event 1: Steam Generator Tube Rupture)

Table 2-1 shows the list of IDHEAS AT-POWER crew failure modes as they were presented in the training and used for testing. Analysts were advised that all crew failure modes should be reviewed for each critical task and a justification should be provided if the crew failure mode was not applicable to a critical task (i.e., if the answer to the question under the guidance column is no). After identifying the applicable crew failure modes for a critical task, analysts would use the crew failure mode decision trees and associated guidance for assessing performance-influencing factors to choose a crew failure scenario for each applicable crew failure mode. Figure 2-3~~Figure 2-3~~ shows a sample crew failure mode decision tree for Crew Failure Mode AP2 (Misread or Skip Step in Procedure).

Table 2-1 IDHEAS AT-POWER Crew Failure Modes

Response Phase	Crew Failure Mode	Guidance
All Phases	AP1: Key Alarm Not Attended To	Does success require alarm response?
	AP2: Misread or Skip Critical Step(s) in Procedure	Is a written procedure being used?
Status Assessment	SA1: Data Misleading or not Available	Does success require data collection to assess plant status?
	SA2: Wrong Data Source Attended To	
	SA3: Critical Data Misperceived	
	SA4: Critical Data Dismissed/Discounted	
	SA5: Premature Termination of Critical Data Collection	Does success require monitoring a critical plant parameter?
Response Planning	RP1: Misinterpret Procedures	Does the success require a decision (e.g., transfer to another procedure or initiate action)?
	RP2: Choose Inappropriate Strategy	Does the procedure allow a choice of strategies?
Execution	E1: Delay Implementation	Does success require responding when a critical value is reached (given the value has been recognized)?
	E2: Critical Data Not Checked/Monitored with Appropriate Frequency	Does success require monitoring for a critical plant parameter as a cue to initiate response?
	E3: Fail to Initiate Execution	Does the task require action on plant systems?
	E4: Fail to Correctly Execute Response (Simple Task)	
	E5: Fail to Correctly Execute Response (Complex Task)	

The decision tree in Figure 2-3~~Figure 2-3~~ is a representation of performance-influencing factors that are important in the evaluation of the Crew Failure Mode AP2 (Misread or Skip Step in Procedure). The decision tree is not an analysis tool; rather, it is a quantification lookup table. The analysts use their qualitative analysis to determine performance-influencing factors levels associated with Crew Failure Mode AP2 in the context of the scenario, and thereby select a path through the decision tree to look up the associated human error probability. Each numbered crew failure scenario has an assigned human error probability value. The human error probabilities are not shown in Figure 2-3~~Figure 2-3~~ because the analysts were not informed of the actual human error probability values until after they completed the testing to avoid having their judgments affected by the actual values of the human error probabilities.

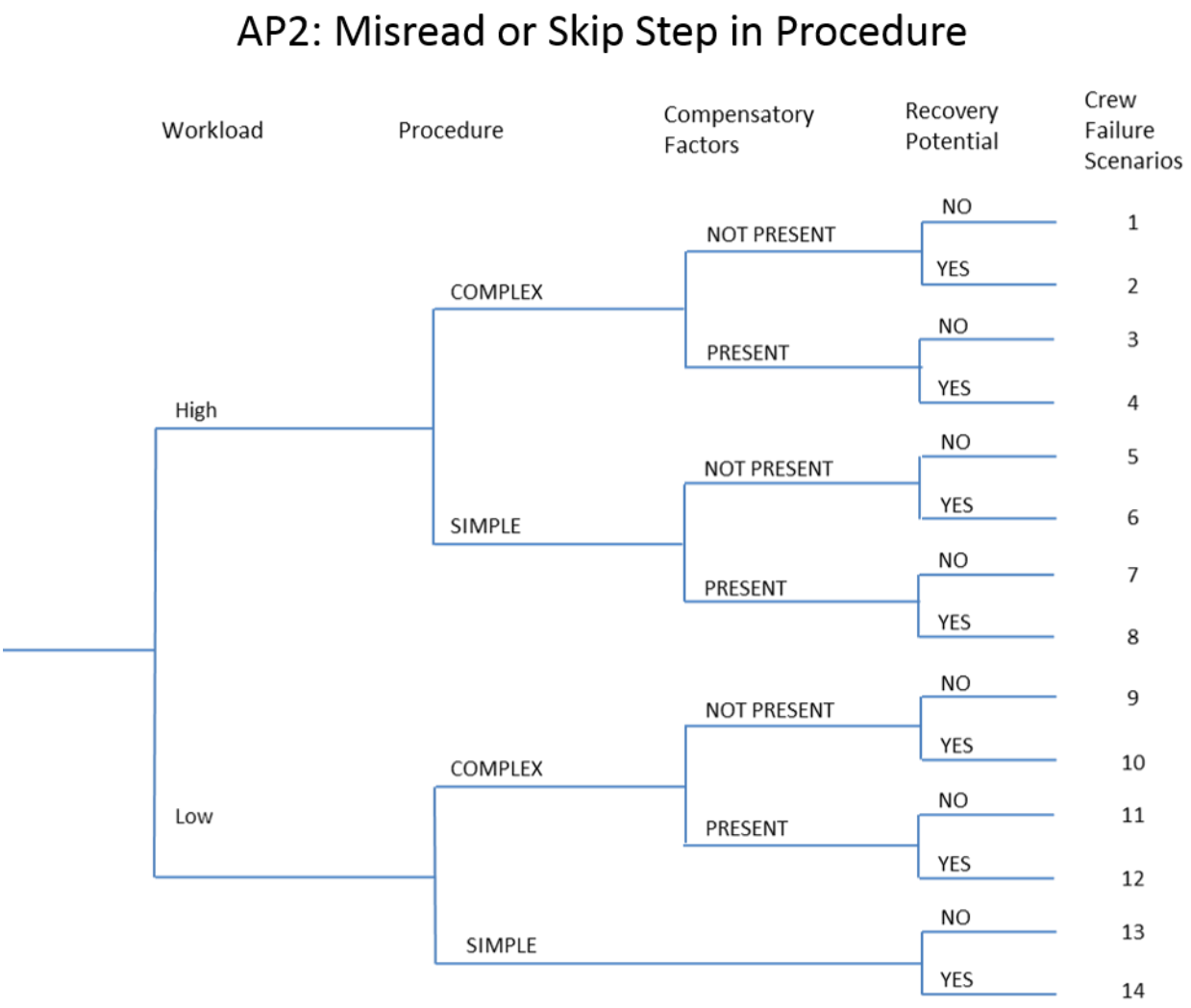


Figure 2-3 Sample Crew Failure Mode Decision Tree for Crew Failure Mode AP2: Misread or Skip Step in Procedure

2.4 Human Reliability Analysis Input and Output

A critical activity in the performance of an HRA is information gathering about the background, training, and experience of the crews and the performance conditions (e.g., human-system interface and job aids such as procedures, availability of cues, and potential distractions). To simulate the information gathering, a designated operator from the project team briefed the analyst teams on the testing scenarios at the end of the training workshop. After the training workshop, the teams had the opportunity to interview the same designated operator to collect additional information about the testing scenarios. The teams were instructed to use the designated operator as a subject matter expert for all questions related to the performance of the crews and the plant. The approach of designating a single operator to answer all operations-related questions was used to limit variability during the information gathering stage of the HRA. Note that the designated operator was not associated with the plants the scenarios came from, so some of the information given to the teams had to be assumed.

The analyst teams also had the opportunity to request clarifications or additional information from the project team. The questions from each team and the answers from the project team were not shared with the other HRA teams to ensure that each team's analyses were independent and not unduly influenced by other team's information gathering, except for a few instances in which the information was decided to be critical to performing the analysis.

An information package (see Appendix A) was compiled for the analyst teams to ensure each team had access to the same information as a basis for their analyses. The package provided descriptions of the scenarios and the human failure events to be analyzed, copies of all training material and the IDHEAS AT-POWER report, and the relevant procedures and other plant information necessary for the teams to perform the analyses.

Although shortened guidance was provided in a separate file to assist the teams in assessing crew failure modes and decision trees, the teams were instructed that the file was not intended to replace the guidance in the method report and the teams should refer to the method report when more guidance was needed.

Appendix B presents the mean human error probabilities associated with each crew failure mode crew failure scenario in IDHEAS AT-POWER. These human error probabilities were not provided to the analysts during the testing to avoid the possibility that the human error probability values would influence the analysts' selection of crew failure scenarios within each decision tree. The sample crew failure mode decision tree in Figure 2-3~~Figure 2-3~~ shows how the decision trees were presented to the analyst teams, with each crew failure scenario assigned a number on the right-hand side of the decision tree. The analyst teams were advised that each crew failure scenario on the crew failure mode decision trees corresponded to a human error probability. Rather than calculating human error probabilities, the teams were instructed to document which crew failure modes and crew failure scenarios they selected for each critical task associated with the human failure event. For example, the designation "AP2-4" corresponds to Crew Failure Scenario 4 on the decision tree for Crew Failure Mode AP2 (Misread or Skip Step in Procedure). After the analyst teams submitted their analysis results and post-analysis questionnaire, the project team calculated the final human error probability of each human failure event and provided this to the analyst teams. Next, the analyst teams were asked to review the final human error probabilities for a consistency check and were given the opportunity to revise their results if the human error probabilities were not consistent with their expectations. None of the teams chose to revise their analyses.

As part of the information package, each analyst team received a template for documenting the HRA, with a sample analysis report using the template. The teams could document their analyses in other formats, but all teams chose to use the template provided. See Appendix C for the sample analysis report using the documentation template.

Each analyst team was also asked to complete a questionnaire after they completed their analysis of the human failure events using IDHEAS AT-POWER. The post-analysis questionnaire had two sections. The first section was intended to collect additional information on each human failure event to assist the project team in evaluating how the analyst teams used IDHEAS AT-POWER. The second section consisted of questions on analysts' overall experience with the method.

2.5 Evaluation Criteria

The study evaluated the results of the testing against the criteria outlined below by comparing across analyst teams and with empirical data when available.

2.5.1 Validity

The study evaluated the validity of IDHEAS AT-POWER by determining whether the method provides a reasonable assessment of human reliability. In other words, a valid method should enable analysts to identify the most likely causes of failure[2] given a human failure event, and consequently derive a human error probability that is appropriate, acceptable, and useful in risk assessment terms. Thus, the evaluation of validity focused on both the qualitative and quantitative information derived from using the method.

The credibility of the evaluation of validity is proportional to the quality of the data used to evaluate validity [9]. Kirwan [9] classified validation of HRA methods into three categories based on the quality of data used. Since validity measures the degree of agreement between the assessment of human reliability and reality, it is best checked with data from real operational contexts relevant to HRA scenarios (e.g., incidents and near misses). Validation against real operational contexts is termed *absolute* or *first order* validation. If other data from less operationally valid contexts are used (e.g., simulator data), the validation is referred to as *approximate* or *second-order* validation. In cases where validation is between one method's predications and another's, rather than comparing method estimates against known HRA data, the validation is referred to as *convergent* or *third-order* validation. The insights from convergent or third-order validation are less credible than those from absolute or approximate validation (first-order or second-order validation, respectively). However, given the sparsity of relevant operational data, convergent validation is worthwhile and may be more practical compared to other types of validation, particularly for well-analyzed scenarios where convergence can be established among several HRA methods. The testing primarily addressed third-order validation, with some opportunities to explore second-order validation given the availability of simulator data associated with Scenarios 1 and 2.

Some of the specific questions the study considered in evaluating validity included:

a) Do the failure causes identified using IDHEAS AT-POWER correspond to the failures observed in real or simulated events?
b) Do the failure causes identified using IDHEAS AT-POWER correspond to those identified by other HRA methods?
c) Are there performance influencing factors identified by IDHEAS AT-POWER that were not identified by empirical data or other HRA methods?
d) Are the human error probabilities using IDHEAS AT-POWER overly optimistic or pessimistic for difficult human failure events?
e) When rank ordered, are the human error probabilities using IDHEAS AT-POWER consistent with rankings of the difficulty of the human failure events?
f) Are the human error probabilities estimated using IDHEAS AT-POWER within the uncertainty bounds of the human error probabilities from empirical data?

[2]In IDHEAS AT-POWER, a failure cause is characterized by the identification of a crew failure mode that leads to the failure of a critical task and the context (performance-influencing factors) resulting from the accident scenario. There could be several failure causes contributing to a human failure event.

g) Do the human error probabilities produced using IDHEAS AT-POWER differentiate between human failure events with different levels of complexity?

2.5.2 Interanalyst Consistency

The study evaluated interanalyst consistency by determining the extent to which different HRA analyst teams produced the same or similar results when using the IDHEAS AT-POWER guidance. Interanalyst consistency was evaluated for both the qualitative analysis and quantitative results (i.e., human error probabilities). Previous benchmark studies [2] have documented concerns with variability between analysts, even when using the same method.

Some of the specific questions considered in evaluating interanalyst consistency included:

a) To what extent do different HRA analyst teams produce the same qualitative analysis, including operational narrative, task analysis, timeline, applicable crew failure modes, performance influencing factors, and recovery potential?
b) To what extent do different HRA analyst teams produce the same quantitative results, including the relative contributions from the applicable crew failure modes, the overall human error probabilities, and human error probability ranking?
c) Do the analyst teams demonstrate the same interpretations of the method guidance?
d) Do the analyst teams document similar justifications for their decisions and conclusions?

2.5.3 Traceability

The study evaluated traceability as the extent to which IDHEAS AT-POWER documentation provided a clear link from the qualitative analysis to the quantitative inputs, and then to the human error probabilities. Traceability should be sufficient to allow for a third party to understand how the analysts derived human error probabilities for each human error event. Traceability is particularly critical in circumstances where there are disagreements in the HRA results because it allows the analysts to identify where and why their results differ.

Some of the specific questions the study considered in evaluating traceability included:

a) Are the analysts' assumptions or the rationales for their decisions (e.g., applicable crew failure modes and performance-influencing factor ratings) clearly documented?
b) Can the source of differences between analyst teams be easily identified in the documentation?

2.5.4 Usability

The study evaluated the usability of IDHEAS AT-POWER in terms of the quality of the analysts' experience with using the method for HRA. Usability can be an important factor affecting whether analysts choose to use the method for real HRA applications.

Some of the specific questions the study considered in evaluating usability included:

a) To what extent is IDHEAS AT-POWER easy to learn and use?
b) How much time is required to analyze a scenario using IDHEAS AT-POWER?
c) What resources are needed to apply the IDHEAS AT-POWER method?
d) Do analysts experience any difficulties when applying IDHEAS AT-POWER?
e) What are the analysts' perceptions of IDHEAS AT-POWER compared to other methods?

f) Would the analysts use IDHEAS AT-POWER in place of their current HRA method of choice?

2.5.5 Utility

The study evaluated the utility of IDHEAS AT-POWER in terms of the extent to which it provided useful information for decisionmaking, including its ability to identify potential error reduction measures. In addition to deriving human error probabilities to inform PRA, the qualitative outputs of HRA can be useful for understanding how human failures may occur, and thereby identify human performance improvement recommendations.

Some of the specific questions the study considered in evaluating utility included:

a) To what extent does IDHEAS AT-POWER provide information that would allow insights for error reduction and other risk management activities? Such information includes where error reduction needs to take place and what needs to be done to achieve improvement in human reliability.
b) To what extent can information from IDHEAS AT-POWER be used to support HRA data collection, analysis, and exchange?

3 ASSESSMENT OF TESTING RESULTS

The testing produced a rich set of qualitative and quantitative data, both of which the study analyzed to identify the strengths and weaknesses of IDHEAS AT-POWER. We paid specific attention to differences across the teams to understand possible contributing factors to variability in HRA results. The quantitative results were examined first in the study to direct the assessment of the qualitative analysis. By tracing back from the observed variability in the quantitative results to its sources, we can understand how the variability arises in the analysis process, whether the variability is caused by the method or by the use of the method. We can then pinpoint areas of concern and determine specific recommendations and solutions to improve the method. In the following sections, overall quantitative results estimated by IDHEAS AT-POWER are first presented with a comparison to the results from NUREG-2156, "The U.S. HRA Empirical Study," [2] and human error probabilities expected by the analyst teams. Next, observations from the qualitative analysis are discussed. Then, a comparison across the analyst teams for each human failure event is presented. Additional insights from the project team regarding the testing results are labeled as "evaluator commentary" and highlighted in boxes throughout the text.

3.1 Overall Quantitative Results Estimated Using IDHEAS AT-POWER

The estimated mean human error probabilities of all human failure events by the five HRA analyst teams are presented in Figure 3-1~~Figure 3-1~~.

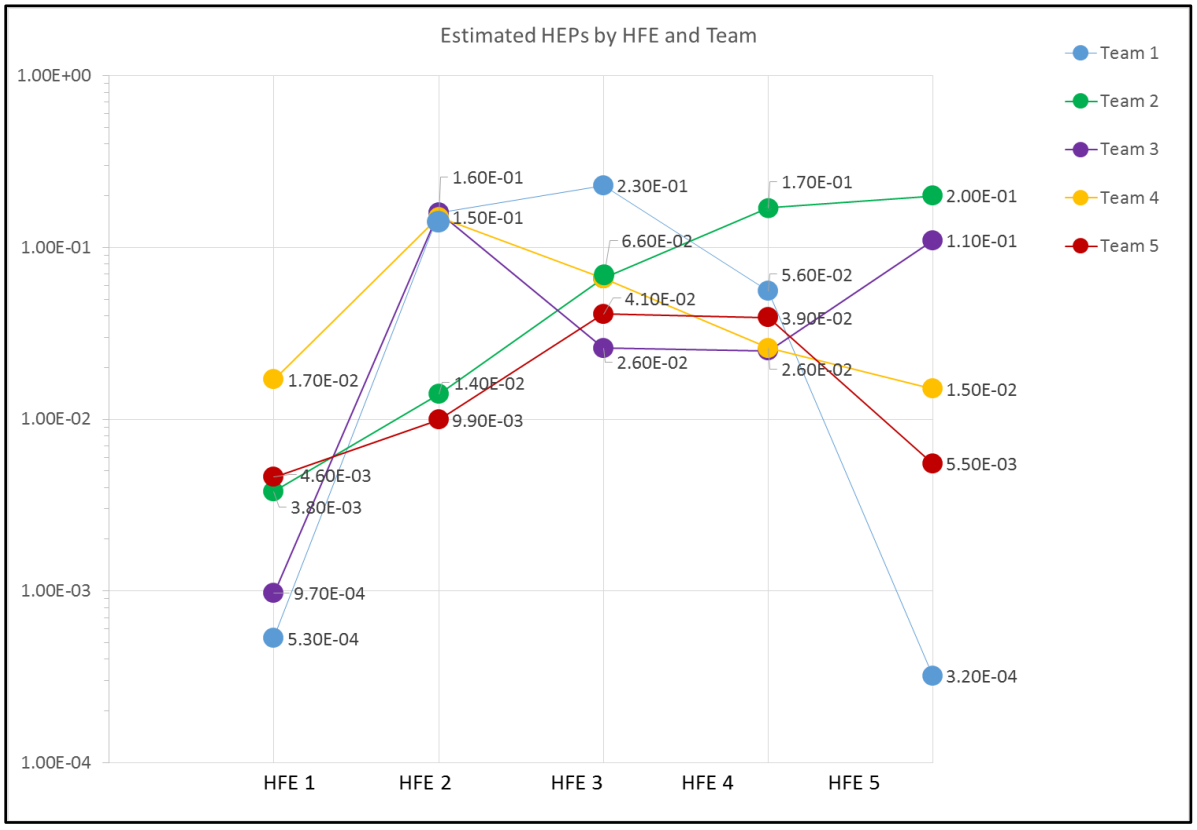


Figure 3-1 Estimated Human Error Probabilities Using IDHEAS AT-POWER by Human Failure Event and Team

3.1.1 Variability in Human Error Probabilities

This section summarizes some observations on the variability in the human error probabilities estimated using IDHEAS AT-POWER. Section 3.1.1 of this report includes a more detailed discussion of the topic.

As can be seen in Figure 3-1~~Figure 3-1~~, there was a certain amount of disagreement among the estimated human error probabilities for each human failure event. The variability of the human error probabilities for Human Failure Event 2, Human Failure Event 3, and Human Failure Event 4 is approximately one order of magnitude, whereas there is significantly more variability for Human Failure Event 1 and Human Failure Event 5. No team estimated consistently conservative or optimistic human error probabilities compared to other teams. The differentiation across human failure events varied across teams. For Team 1, there is a difference of approximately three orders of magnitude between the highest and the lowest human error probabilities. In contrast, the human error probabilities of all human failure events of Teams 4 and 5 fall within a range of approximately one order of magnitude.

Although all the HRA teams identified operator response associated with Human Failure Event 1 to be the easiest, the human error probabilities of Human Failure Event 1 showed variability of approximately two orders of magnitude. One reason for Team 4 being significantly higher than the other four teams is that, in contrast to other teams, Team 4 estimated that identification of steam generator tube rupture would not be easy with available cues. Team 4 seemed to base this idea on its interpretation of the information from the interview with the designated operator. This resulted in a higher final human error probability for Team 4. Team 3 produced a lower human error probability partly because the team credited recovery for the execution of cooldown and depressurization, which is a complex control action. However, the method guidance advises that recovery should not be applied in the case of control actions. If Team 3 had not credited recovery, their final human error probability would have been one order of magnitude higher and comparable to Team 5's final human error probability. Team 1 estimated a lower human error probability than other teams in part because they identified cooldown and depressurization as a straightforward action that was unlikely to fail.

For Human Failure Event 2, Teams 1, 3 and 4 obtained approximately the same human error probability. A closer look at their analyses revealed that the five teams agreed on the same dominating crew failure mode, namely Crew Failure Mode SA1 (Data Misleading or Not Available). However, their differences in choosing the path (i.e., set of performance-influencing factors values) on the same decision tree caused the human error probabilities of Teams 2 and 5 to be about one order of magnitude lower than those of Teams 1, 3, and 4.

The human error probabilities of Human Failure Event 3 fall in a relatively narrow range. One result that is worth noting is that Teams 2 and 4 obtained the same human error probability with the selection of the same set of crew failure modes and decision tree paths. Team 1 and Team 3 selected different crew failure modes that dominated their final human error probabilities for Human Failure Event 3. Team 1 selected Crew Failure Mode SA1 (Data Misleading or Unavailable) as a failure mode for the identification of loss of seal cooling and Team 3 selected Crew Failure Mode E3 (Failure to Initiate Execution) as a failure mode for opening FCV-626. A review of the teams' justifications for Crew Failure Mode SA1 and Crew Failure Mode E3 suggested that the teams may have misinterpreted the guidance for selecting those crew failure modes.

The human error probabilities of Human Failure Event 4 also fall in a relatively narrow range with Teams 3 and 4 producing approximately the same human error probability. However, the teams did not agree on the dominating crew failure modes.

Although the teams had a consensus on the procedural path and the tasks that operators would need to perform for successful response associated with Human Failure Event 5, the human error probabilities significantly deviated from each other, leading to approximately three orders of magnitude difference. The teams appeared to have different understandings of the scenario. For example, there were differences in the assessment of whether workload was high or low, and whether the crews would experience time pressure to cooldown and depressurize the reactor within the time available. These differences in assessment were partly due to differences in how the teams interpreted the human failure event definition. One team interpreted successful crew response as requiring the crew to *initiate* cooldown and depressurization within the 2-hour time window, which was the original intended definition of the human failure event. However, because the definition was ambiguous, other teams relied on information from the operator interviews to determine the stopping point in the procedures for when the crew achieved a successful response. Information provided during the operator interviews led the teams to assume that successful response required the operating crew to *complete* cooldown and depressurization to below 400°F within a 2-hour time window, which inadvertently increased the potential time pressure on the crew. This led to substantial differences in the selection of crew failure modes and performance-influencing factors, and thereby impacted the final human error probabilities.

3.1.2 Comparison to U.S. Empirical Study Data

Figure 3-2~~Figure 3-2~~ shows the estimated human error probabilities for Human Failure Event 1 and Human Failure Event 2 using IDHEAS AT-POWER in the current study versus other HRA methods from data taken from the U.S. Empirical Study. The solid dots connected by solid straight lines represent estimates using IDHEAS AT-POWER; the open circles represent estimates from the U.S. Empirical Study [2]. The points connected by dotted lines represent the 5th and 95th percentile uncertainty bounds for the two human failure events. The bounds were derived through a Bayesian update with a noninformative prior (Jeffery's prior) using the data from the four crews who simulated the responses associated with the human failure events on a simulator as part of the U.S. Empirical Study.

As can be seen in Figure 3-2~~Figure 3-2~~, the majority of the human error probability estimates using IDHEAS AT-POWER fall within the 5th and 95th percentile uncertainty bounds, with one human error probability for Human Failure Event 1 slightly below the 5th percentile. Since they are very large uncertainty intervals, based as they are on a small sample with no failures, they provide some, but only weak, evidence that the analyst teams did not significantly under- or over-estimated the two human failure events using IDHEAS AT-POWER. Furthermore, the human error probabilities of the two human failure events seem to be comparable to estimates from NUREG-2156, "The U.S. HRA Empirical Study."

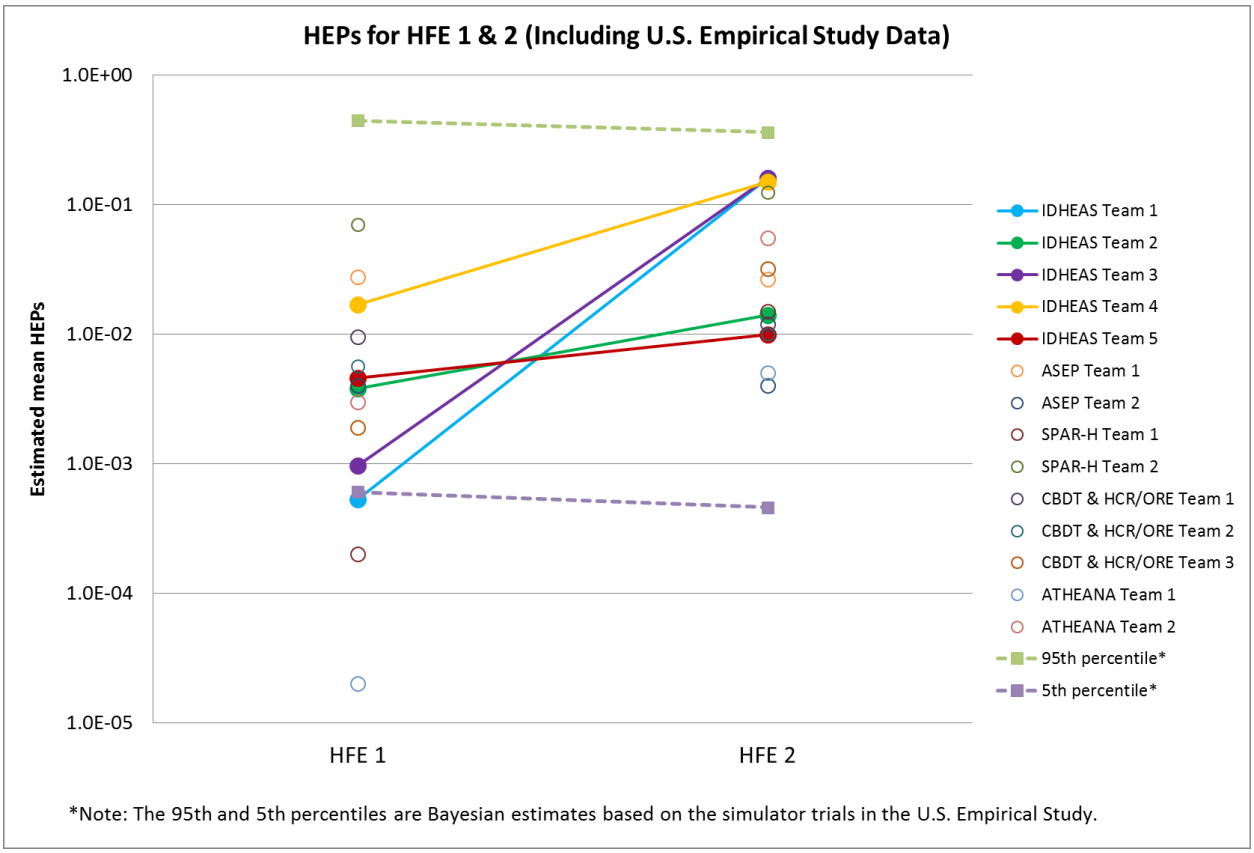


Figure 3-2 Estimated Human Error Probabilities for Human Failure Event 1 and Human Failure Event 2 (including U.S. Empirical Study Data)

3.1.3 Comparison of Estimated Human Error Probabilities to Expected Human Error Probabilities

In addition to the human error probabilities estimated using IDHEAS AT-POWER, each team was asked to provide a point estimate of the expected human error probability for each human failure event. The expected human error probability was solicited after the team completed their analysis of the human failure events, but before they received the calculation of the estimated human error probabilities for each of the human failure events using IDHEAS AT-POWER. Thus, the expected human error probabilities were a quantitative indicator of the team's subjective assessment of operator performance, while they were blind to the human error probabilities associated with the crew failure scenarios they selected using IDHEAS AT-POWER.

The comparison of the expected human error probabilities against the estimated human error probabilities served as an opportunity for the analyst teams to perform a consistency check on their analyses, particularly with respect to the relative ordering of the human error probabilities. Unexpected differences in the relative ordering of the human error probabilities should prompt a more detailed review of the analyses to ensure that the differences are not due to errors in documentation or that the analyses explain why analysts' initial judgments were incorrect. The analyst teams could review and amend their analyses as part of this consistency check; none of the teams chose to change their analyses.

Figure 3-3~~Figure 3-3~~ presents the expected human error probabilities. No team was more consistently conservative or optimistic than others. All teams agreed that the response to Human Failure Event 1 was the least difficult, and the expected human error probabilities for Human Failure Event 1 were within one order of magnitude of each other. For Human Failure Events 2, 3, and 5, the variability across teams was more than one order of magnitude. Teams 1, 4, and 5 were fairly consistent in their expectations across the human failure events. Furthermore, they expected comparable human error probabilities between Human Failure Events 2 and 5.

The lack of consensus in the expected human error probabilities suggests that the teams had different perceptions of how the crew challenges (i.e., operational problems), scenario dynamics, and contextual factors may influence performance. For example, it was observed that the analysts sometimes made different assumptions when information was insufficient, when they had different operator expectations, or when they interpreted differently the information obtained from operator interviews. Examples included the analyst teams' different expectations regarding the procedural path operators would take in Human Failure Event 3, and the different interpretations of the criteria for successful crew response in Human Failure Event 5.

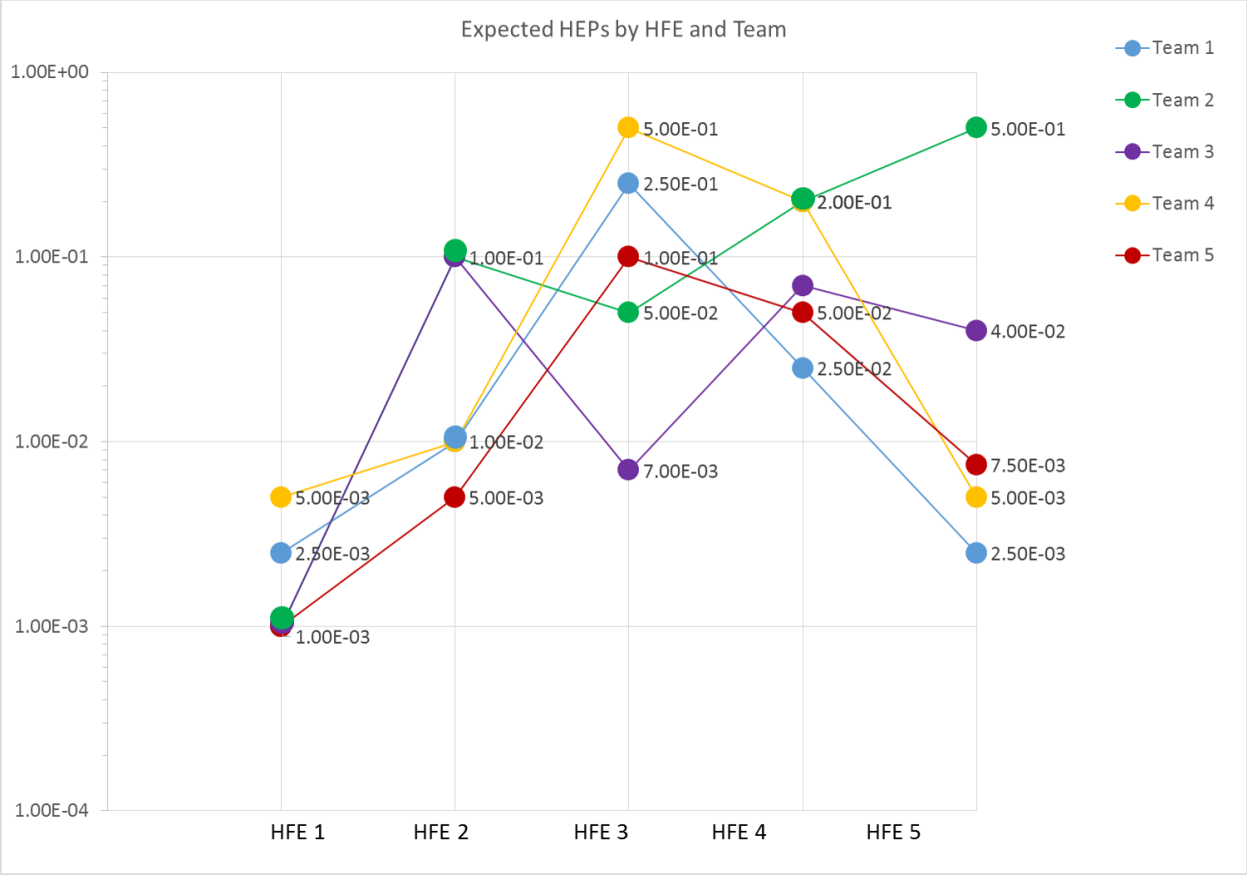


Figure 3-3 Expected Human Error Probability by Human Failure Event and Team

Figure 3-4~~Figure 3-4~~ shows a comparison of the teams' estimated human error probabilities and expected human error probabilities. In most cases, the differences between the expected human error probabilities and the estimated human error probabilities were less than one order of magnitude. This suggests that IDHEAS AT-POWER produced human error probability estimates that were reasonably consistent with HRA analysts' expectations.

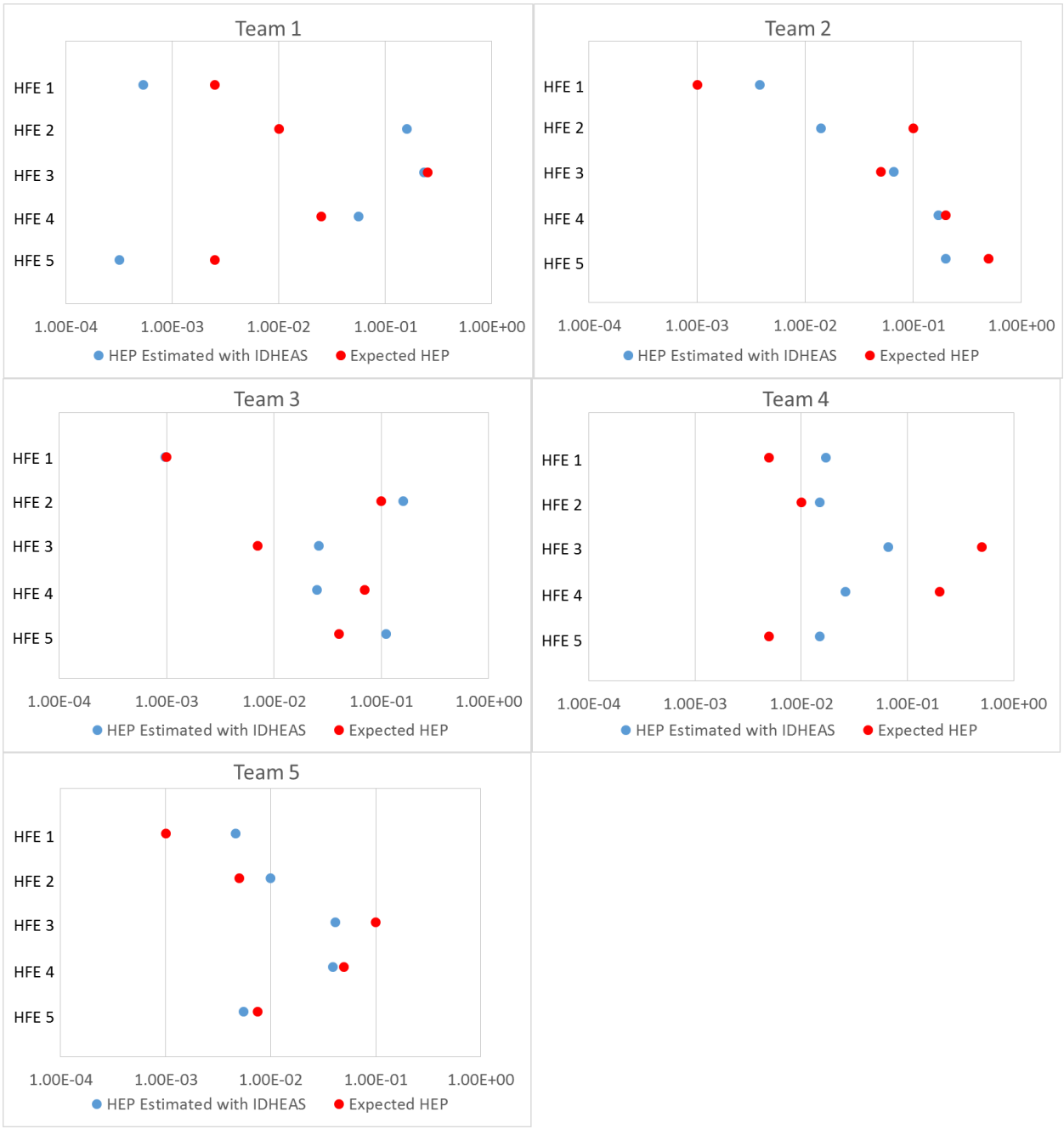


Figure 3-4 Comparison of Estimated and Expected Human Error Probabilities

3.2 Observations from the Qualitative Analysis

The qualitative analysis includes developing operational narratives, constructing and explaining crew response diagrams, creating timelines, and performing task analyses. The development of an operational narrative enables analysts to focus on the unfolding of a scenario, the evolving perspective of operators, and how each required task is performed and may fail as a function of the scenario evolution. Such information is the basis for evaluating which crew failure modes are applicable, and the characterization of the corresponding performance-influencing factors. Rather than examining a set of characteristics of the human failure event (e.g., by assessing procedural guidance and other performance-influencing factors at an overall level), the construction of crew response diagrams and timelines forces analysts to carefully parse procedures and collect HRA-relevant information to thoroughly understand the scenario context. That is, the understanding of the human failure event is developed explicitly in the analysis process. This approach can enable many scenario-specific timing and performance issues to be identified and treated within the analysis process, which is necessary and important for obtaining rich insights into the dynamics of complex scenarios.

It was observed that the analyst teams' interviews with the designated operator were oriented towards identifying: (1) procedural success paths, critical tasks, and recovery potential; (2) the plant status trajectory in terms of the timing of cues and other plant process parameters that are required for operators to correctly perform the required response or to realize an opportunity for recovery; and (3) the time at which operators were expected to reach critical steps in the procedure. Analysts' reliance on the designated operator appeared to vary with their knowledge of procedures, operations, and scenarios, which resulted in some teams producing qualitative analyses with relatively richer, more detailed content than others.

Overall, there tended to be relatively less variability in the qualitative analyses of human failure events that involved less difficult operator response (i.e., Human Failure Event 1) and other human failure events that also had well-defined procedural success paths (i.e., Human Failure Events 2 and 5). The human failure events for which there were multiple potential procedural success paths (i.e., Human Failure Events 3 and 4) had more interanalyst variability, due to (1) differences in analysts' judgment and assumptions about how relevant cues would be perceived, which procedure would be entered, and how it would be entered, and (2) analysts' uncertainty regarding certain plant parameters and how operators would respond to potentially ambiguous procedures. For Human Failure Events 1 and 2, the identified procedural paths and performance drivers were consistent with the simulator data observed in the U.S. Empirical Study. For Human Failure Event 5, although the teams had a consensus on the procedural path and the critical tasks, there was considerable disagreement on main performance drivers, as evidenced in the selection of crew failure modes and performance-influencing factor ratings. Some of these differences were likely due to different understandings of the scenario, particularly on how the scenario developed in such a way that reactor coolant pump seal failure occurred. For example, it can make a difference whether the reactor coolant pump seal failure is assumed to have resulted from a prior failure of the crew to restore cooling or a mechanical failure. The teams were told to treat Human Failure Events 3, 4, and 5 as independent, but since they are clearly not independent, this almost certainly influenced how different analysts viewed the accident progression.

The teams differed in how they modeled execution tasks. In IDHEAS AT-POWER, an execution task is intended to be addressed in an integral manner rather than by assessing each of the individual subtasks (i.e., in contrast to some other HRA methods, like THERP). For example, in a steam generator tube rupture scenario, the operator would need to perform reactor coolant

system cooldown and depressurization and then control reactor coolant system pressure after the ruptured steam generator is isolated. Since these tasks are all part of one procedure directing the execution, these tasks should be treated and quantified holistically as one task in the IDHEAS AT-POWER approach. However, some teams modeled these types of execution subtasks separately.

Differences arose among crew response diagrams in terms of how tasks were grouped together, or whether a task was explicitly considered when it was assessed as having a low likelihood of failure. For example, all teams seemed to agree that identification of the ruptured steam generator was not likely to fail in Human Failure Event 1, but they treated the task differently. The first approach was to model the task explicitly, the second was to treat the task as an assumed success and not model it, and the third approach was to implicitly model the task by combining it with the identification of the steam generator tube rupture. However, the different approaches did not seem to have a significant impact on the quantitative results because each team considered the failure probability of this task to be low compared to those of other tasks.

The study also observed differences in analysts' assumptions when there was uncertainty about which actions operators would take. In Human Failure Events 3 and 4, the choice of some operator actions depended on the operators' response to specific plant parameters or their interpretations of the procedures. Analysts had to make assumptions about those actions, which resulted in variations in the analysts' crew response diagram construction and crew failure mode selection. See Section 4.2.1 and Section 4.6.2 for additional discussion of this issue of analyst judgment in method application.

Since the probability of misreading or skipping a step in a procedure is already accounted for in the failure probability in the execution crew failure modes, Crew Failure Mode AP2 should not be used in cases where the procedural steps associated with the task were simply directing the execution. However, all teams, including the project team (Team 5), which included IDHEAS AT-POWER developers, used Crew Failure Mode AP2 (Misread or Skip Step in Procedure) inappropriately and contrary to the method guidance when modeling execution tasks.[3]

Evaluator commentary: The overuse of Crew Failure Mode AP2 may be due to a combination of factors, such as the misnomer of labeling the crew failure mode as AP for "all phases," the caution against using AP2 was not highly visible in the guidance, and the caution was not emphasized during training.

3.3 Interanalyst Comparisons by Human Failure Event

The analyses of each human failure event by different analyst teams were compared to (1) identify the strengths and weaknesses of IDHEAS AT-POWER independent of analyst-specific effects, and (2) reveal where in the analysis process variability in HRA results can occur and how it can occur. Each comparison includes a discussion of the human error probabilities estimated using IDHEAS AT-POWER versus the expected human error probabilities estimated by the analyst teams. Then, the observed differences on critical tasks, procedural paths, recovery modeling, and assessment of crew failure modes and performance-

[3] Note that the inappropriate use of Crew Failure Mode AP2 (Misread or Skip Step in Procedure) has been corrected in the analyses presented in Appendix C.

influencing factors are presented with a discussion of the underlying methodological and guidance limitations that permitted the differences to arise.

3.3.1 Human Failure Event 1

3.3.1.1 Estimated vs. Expected Human Error Probabilities

All the teams expected Human Failure Event 1 to have a relatively low probability of failure, with expected human error probability values ranging from 1E-03 to 5E-03 (See Figure 3-5~~Figure 3-5~~). The teams' estimated human error probabilities ranged from 1.7E-02 to 5.4E-04 and were within one order of magnitude of their expected human error probabilities for Human Failure Event 1. In particular, Team 3's estimated human error probability was a very close match to their expected human error probability. Team 1 had the lowest estimated human error probability and Team 4 had the highest estimated human error probability.

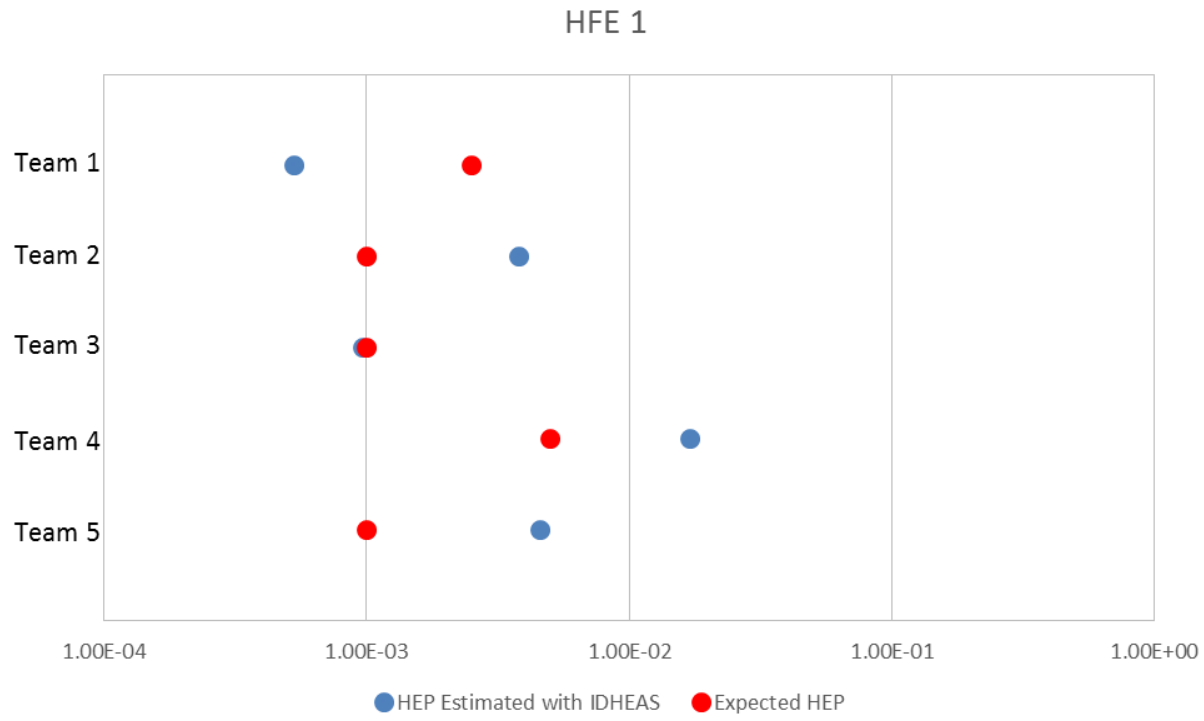


Figure 3-5 Comparison of Estimated and Expected Human Error Probabilities for Human Failure Event 1

3.3.1.2 Critical Tasks and Procedural Paths

The five teams identified some or all of the following as critical tasks that the operating crews would need to accomplish for a successful response.

- Critical Task 1: Diagnose steam generator tube rupture
- Critical Task 2: Identify ruptured steam generator

- Critical Task 3: Isolate ruptured steam generator

- Critical Task 4: Cooldown and depressurize the reactor coolant system

depicts a comparison of each team's analysis for Human Failure Event 1. The table includes key highlights from each team's scenario analysis, a list of the crew failure modes and crew failure scenarios chosen by each team for the critical tasks that they modeled and analyzed, and their final estimated human error probability. Refer to Appendix B for a complete list of the crew failure scenarios associated with each crew failure mode decision tree and their corresponding human error probabilities.

All the teams seemed to be familiar with the scenario. They agreed on the procedural path, the cues for diagnosing steam generator tube rupture, and what the operators need to do in response to a steam generator tube rupture. The differences appeared in task decomposition and execution task modeling, as can be seen in the analysis comparison in Table 3-1.

- Although Teams 1, 2, and 3 recognized that the operators would need to identify the ruptured steam generator, they did not model it explicitly and seemed to combine it implicitly with Critical Task 3.

- Team 2 decomposed Critical Task 3 into two subtasks: 1) isolate ruptured steam generator and 2) stop auxiliary feedwater flow to ruptured steam generator. On the other hand, Team 3 combined Critical Tasks 3 and 4 into one critical task.

- Teams 2 and 4 decomposed Critical Task 4 into three subtasks. Because the reactor coolant system cooldown and depressurization only involved execution (and not status assessment or response planning), the IDHEAS AT-POWER guidance suggests treating the task holistically. The result of decomposing Critical Task 4 is repeated use of the execution crew failure modes for what can be considered a single complex control action.

- Analysts disagreed on whether to categorize Critical Task 3 as a simple or complex execution. In addition, although Teams 2 and 4 both chose to decompose the execution of cooldown and depressurization into three subtasks, they did not agree on whether the act of depressurizing the reactor coolant system was a simple or complex execution.

Evaluator commentary: The guidance for the execution crew failure modes could be improved to provide more examples of the types of tasks that are simple versus complex.

3.3.1.3 Recovery Modeling

All the teams identified a recovery path for Critical Task 1. Teams 1 and 2 identified recovery for Critical Task 3. Team 5 credited recovery for Critical Tasks 2 and 3 but did not identify them in the task analysis or include them on their crew response diagram (see Appendix C-1). Teams 1 and 3 identified recovery for Critical Task 4. However, this was not necessary because the teams considered cooldown and depressurization as a complex control action, which, per method guidance, does not have recovery.

Table 3-1 Comparison of Teams' Analysis for Human Failure Event 1

HFE 1: Steam Generator Tube Rupture									
Team		*Critical Tasks*							*HEP*
		Diagnose SGTR	**Identify Ruptured SG**	**Isolate Ruptured SG**		**Cooldown and Depressurize RCS**			
1	**Analysis**	Recovery at E-0, Step 22. Not quantified.	Low likelihood of failure to identify SG. Not quantified.	Isolation modeled as simple execution. Recovery at E-3, Step 14.		Modeled as one control action with recovery.			**5.3E-04**
	CFMs			AP2-14 (1.2E-04) E3-5 (1.4E-04) E4-8 (1.6E-06)		AP2-14 (1.2E-04) E3-5 (1.4E-04) E5-16 (1.0E-05)			
2	**Analysis**	Recovery at E-0, Step 22.	Identification not explicitly modeled.	Recovery at E-3, Step 4a.	Stop AFW flow modeled separately.	Cooldown. Complex execution. Recovery at E-3, Step 15a.	Depressurize. Complex execution.	Control RCS pressure. Complex execution.	**3.8E-03**
	CFMs	AP2-14 (1.2E-04)		AP2-14 (1.2E-04) E3-5 (1.4E-04) E5-16 (1.0E-05)	**AP2-13 (8.2E-04)** E3-5 (1.4E-04) E5-15 (8.0E-05)	AP2-14 (1.2E-04) E3-5 (1.4E-04) E5-16 (1.0E-05)	**AP2-13 (8.2E-04)** E3-5 (1.4E-04) E5-15 (8.0E-05)	**AP2-13 (8.2E-04)** E3-5 (1.4E-04) E5-15 (8.0E-05)	
3	**Analysis**	Recovery at E-0, Step 22.	Identification not explicitly modeled.	Isolation of ruptured SG and cooldown modeled as one node. Recovery modeled for controlling pressure (E-3, Step 24).					**9.7E-04**
	CFMs	AP2-12 (9.7E-05) SA3-7 (1.3E-04)		AP2-12 (9.7E-05) SA3-7 (1.3E-04) E3-5 (1.4E-04) E5-8 (3.8E-04)					
4	**Analysis**	Radiation alarms may have cleared. Two recovery paths (E-0, Step 31; E-0, Step 23).	Identify and Isolate SG modeled as one node, but two critical tasks.	Isolation modeled as simple execution.		Cooldown. Complex execution.	Depressurize. Simple execution.	Control RCS pressure. Complex execution.	**1.7E-02**
	CFMs	AP2-14 (1.2E-04) **SA1-5 (9.6E-03)** SA3-12 (3.4E-05) RP1-8 (N/A)	AP2-13 (8.2E-04) SA2-15 (5.2E-04)	E3-5 (1.4E-04) E4-7 (9.3E-06)		E3-5 (1.4E-04) E5-7 (3.8E-03)	SA3-15 (1.3E-05) E3-5 (1.4E-04) E4-7 (9.3E-06)	**AP2-11 (1.3E-03)** E3-5 (1.4E-04) E5-15 (8.0E-05)	
5	**Analysis**	Recovery at E-0, Step 22.		Complex execution.		Complex control action.			**4.6E-03**
	CFMs	AP2-14 (1.2E-04)	AP2-14 (1.2E-04)	AP2-14 (1.2E-04) E1-7 (1.7E-05) E3-5 (1.4E-04) E5-15 (8.5E-05)		AP2-14 (1.2E-04) E1-7 (1.7E-05) E3-5 (1.4E-04) **E5-7 (3.8E-03)**			

Note. The following crew failure modes were used by one or more teams in analyzing Human Failure Event 1: AP2 (Misread or Skip Step in Procedure); SA1 (Data Misleading or Not Available); SA2 (Wrong Data Source Attended To); SA3 (Critical Data Misperceived); RP1 (Misinterpret Procedures); E1 (Delay Implementation); E3 (Fail to Initiate Execution); E4 (Fail to Correctly Execute Response for Simple Task); E5 (Fail to Correctly Execute Response for Complex Task). The number after the crew failure mode label indicates the crew failure scenario chosen on the crew failure mode decision tree (e.g., AP2-14 corresponds to crew failure scenario 14 on the decision tree for AP2). Refer to Appendix B for a complete list of the human error probabilities associated with each crew failure mode decision tree. Crew failure modes in bold indicate that the crew failure mode was a main contributor to the final human error probability.

3.3.1.4 Assessment of Crew Failure Modes and Performance-Influencing Factors

The five teams' assessment of crew failure modes and performance influencing factors for Human Failure Event 1 is summarized in Table 3-1.

3.3.1.4.1 Critical Task 1: Diagnose Steam Generator Tube Rupture

Team 1 did not quantify Critical Task 1 as they argued that the failure probability was negligible. This is consistent with the results from three of the other teams as they estimated a low probability for failing Critical Task 1. In contrast, Team 4 argued that it might be challenging to identify the steam generator tube rupture because steam generator tube rupture cues (i.e., radiation alarms) might have cleared by the time the operators reach the procedure step to check the cues, which was indicated in the team's interview with the designated operator. This resulted in Team 4 selecting Crew Failure Mode SA1 (Data Misleading or Not Available) and crew failure scenario 5 with a moderate failure probability (9.6E-03), which was the primary driver for their final human error probability.

All the teams that quantified Critical Task 1 used Crew Failure Mode AP2, "Misread or Skip Step in Procedure." However, Team 3 assessed the procedure as complex (AP2-12), whereas the other teams assessed the procedure as simple (AP2-14), but the failure probabilities associated with the crew failure scenarios were approximately the same; thus, the different assessment of procedure complexity did not significantly impact the final human error probabilities.

Evaluator commentary: The project team noted that the probability associated with crew failure scenario AP2-12 (9.7E-05) is lower than the probability associated with crew failure scenario AP2-14 (1.2E-04). This means that a complex procedure with compensatory factors has a lower probability of failure than a simple procedure with no compensatory factors needed. This suggests that a review might be necessary to determine the reasonableness of the failure probabilities associated with crew failure scenarios.

Team 4 identified two crew failure modes for Critical Task 1 that included workload as a performance-influencing factor (Crew Failure Mode AP2 and SA3). However, Team 4 rated workload to be high for Crew Failure Mode SA3 (Critical Data Misperceived), but low for Crew Failure Mode AP2 (Misread or Skip Step in Procedure). Their justification indicates that workload would be low for Crew Failure Mode AP2 because the operators are only using one procedure, whereas workload would be high for Crew Failure Mode SA3 because operators have multiple alarms that may need their attention.

Evaluator commentary: The choice of high workload for this scenario was not consistent with the intent of the method guidance. Although there were multiple alarms, the alarms were not in excess of what operators would experience in training and all the alarms were contributing to a correct plant situation assessment. The presence of multiple alarms would not exceed nominal workload levels expected in a transient scenario.

3.3.1.4.2 Critical Task 2: Identify Ruptured Steam Generator

Teams 1, 2, and 3 did not quantify Critical Task 2 as this task was implicitly combined with Critical Task 3. Teams 4 and 5 both selected Crew Failure Mode AP2 (Misread or Skip Step in Procedure) but did not agree on whether there was recovery potential for Critical Task 2. This resulted in Team 4 selecting crew failure scenario AP2-13, whereas Team 5 selected AP2-14. Note that Team 5 argued that there were multiple cues and thus credited recovery on the

selected crew failure mode decision tree but did not identify the recovery in their crew response diagram. This difference in the identification of recovery potential resulted in a difference of nearly one order of magnitude in the failure probability for Critical Task 2.

3.3.1.4.3 Critical Tasks 3: Isolate Ruptured Steam Generator and Critical Task 4: Reactor Coolant System Cooldown and Depressurization

As discussed above, there was significant variability in how the teams chose to model Critical Tasks 3 and 4 in terms of task decomposition. In addition, there was variability in whether teams chose to model Critical Tasks 3 and 4 as simple or complex execution actions. Team 2, 3, and 5 modeled Critical Task 3 as a complex execution based on their interpretation of the criteria for determining whether an action was complex rather than simple, whereas Team 1 and 4 modeled it as a simple execution. Team 4 modeled part of Critical Task 4 (i.e., reactor coolant system depressurization) as a simple execution, whereas the other teams modeled Critical Task 4 as a complex execution.

Team 1 thought that the complex execution of Critical Task 4 was straightforward, as evidenced by their selection of Crew Failure Mode E5 (Failure to Correctly Execute Complex Task), crew failure scenario 16. In contrast, Teams 3 and 5 chose E5-7 and E5-8, respectively, indicating that the complex execution of Critical Task 4 was not straightforward. This caused the Team 1's failure probability to be one order of magnitude lower than Team 3's and two orders of magnitude lower than Team 5's. Note that Team 1 indicated they were not clear on how to answer the reference questions to evaluate this performance-influencing factor.

Both Teams 1 and 3 credited recovery for Critical Task 4, which is not consistent with method guidance on recovery modeling for complex control actions. If Team 3 had not credited recovery, Team 3's final human error probability would have been one order of magnitude higher and comparable to Team 5's final human error probability.

All teams selected Crew Failure Mode E3 (Failure to Initiate Execution) and agreed that Critical Task 4 is an immediate action, thereby selecting the lowermost path on the decision tree (E3-5). Note that the failure probability associated with E3-5 (1.4E-04) is one order of magnitude higher than the failure probabilities produced by other execution crew failure modes and dominates Team 1's final human error probability for Human Failure Event 1. In other words, if Team 1 had simply screened out Crew Failure Mode E3, Team 1's execution human error probability would have been one order of magnitude lower.

Evaluator commentary: This raises the question of whether the immediacy performance-influencing factor should be considered a screening question for Crew Failure Mode E3 rather than included as an option on the decision tree.

3.3.2 Human Failure Event 2

3.3.2.1 Estimated vs. Expected Human Error Probabilities

The estimated human error probabilities show a variability of approximately one order of magnitude and are fairly consistent with the expected human error probabilities (Figure 3-6~~Figure 3-6~~). All teams agreed that this human failure event should be dominated by the diagnosis human error probability.

Teams 1, 3, and 4 obtained approximately the same human error probability. A closer look at their analyses revealed that the five teams agreed on the same dominating Crew Failure Mode SA1 (Data Misleading or Not Available). However, the teams' choices of different paths on the decision tree for Crew Failure Mode SA1 caused the human error probabilities of Teams 2 and 5 to be about one order of magnitude lower than those of Teams 1, 3, and 4, which is an indication of the sensitivity due to binary nature of the decision tree. It should be noted that Team 4 seemed to have misinterpreted some performance-influencing factors associated with the crew failure mode.

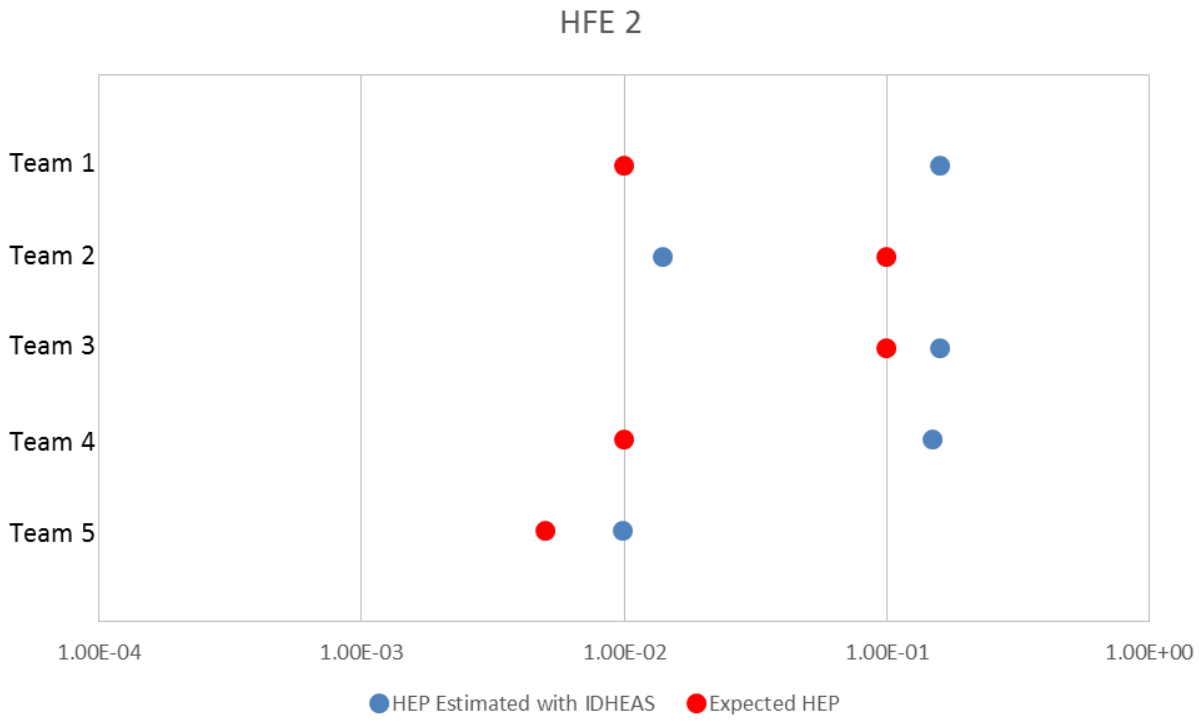


Figure 3-6 Comparison of Estimated and Expected Human Error Probabilities for Human Failure Event 2

3.3.2.2 Critical Tasks and Procedural Paths

The five teams identified the following critical tasks (see Table 3-2~~Table 3-2~~).

- Critical Task 1: Enter ES-01 from E-0 and monitor critical safety function status trees
- Critical Task 2: Identify total loss of feedwater (TLOFW) and enter FRH-1
- Critical Task 3: Implement feed and bleed (F&B)

Table 3-2 Comparison of Teams' Analysis for Human Failure Event 2

HFE 2: Total Loss of Feed Water with Misleading Indicator						
Team		*Critical Tasks*				*HEP*
		Enter ES-01 & Monitor CSF Status Trees	**Identify TLOFW & Enter FRH-1**	**Implement Feed & Bleed**		
1	**Analysis**	Low failure likelihood. Not quantified.	Two monitoring tasks (i.e., SG NR level and AFW flow) modeled together.	Initiate F&B at Step 10.		**1.6E-01**
	CFMs		AP2-14 (1.2E-04) **SA1-4 (1.5E-01)**	AP2-14 (1.2E-04) E1-4 (6.5E-03) E3-5 (1.4E-04) E4-8 (1.6E-06)		
2	**Analysis**		Recovery for control AFW flow (ES-01, Step 8c).	Notes that transitioning from Step 2 to Step 10 is required, but not critical because Step 10 will eventually be reached. Recovery at FRH-1, Step 15.		**1.4E-02**
	CFMs	AP2-13 (8.2E-04)	AP2-13 (8.2E-04) **SA1-5 (9.6E-03)** SA3-15 (1.3E-05) RP2-8 (9.3E-04)	AP2-13 (8.2E-04) RP2-8 (9.3E-04) E3-5 (1.4E-04) E5-16 (1.0E-05)		
3	**Analysis**	Manual trip included as critical action prior to entry into ES-01. Recovery at E-0, Step 4b or Step 8.	Recovery possible due to STA monitoring of CSF status trees.	Recovery at FRH-1, Step 11 and 13.		**1.6E-01**
	CFMs	AP2-14 (1.2E-04) SA3-16 (1.3E-05) RP1-8 (N/A)	AP2-8 (1.5E-04) **SA1-4 (1.5E-01)** SA3-12 (3.4E-05) SA4-8 (2.5E-03) SA5-4 (5.1E-03) RP1-4 (5.1E-03)	AP2-14 (1.2E-04) SA3-16 (1.3E-05) RP1-8 (N/A) E3-5 (1.4E-04) E5-16 (1.0E-05)		
4	**Analysis**	Start monitoring CSFs later in ES-01.	Knowledge-based behavior at Step 22 of ES-01.	Initiate F&B from CIP. SI Actuation is 1st critical task. Steps 10-13 modeled as recovery.	Open PORVs modeled as 2nd critical task in same node.	**1.5E-01**
	CFMs	AP2-13 (8.2E-04) SA3-11 (1.6E-04)	AP2-7 (1.0E-03) **SA1-6 (1.1E-01)** SA3-9 (5.7E-03) RP2-5 (3.3E-02)	E3-5 (1.4E-04) E4-8 (1.6E-06)	E3-5 (1.4E-04) E4-4 (1.6E-06)	
5	**Analysis**	Assumed success. Not quantified.	Monitoring SG NR level and AFW flow modeled separately. Recovery at ES-01, Step 8.	Model transfer from Step 2 to Step 10 as separate task. Recovery at FRH-1, Step 9.	Initiate F&B at Step 10. Recovery at FRH-1, Step 11 and 13.	**9.9E-03**
	CFMs		SA2-16 (5.2E-05) SA3-16 (1.3E-05) **SA1-5 (9.6E-03)**	AP2-14 (1.2E-04) SA3-16 (1.3E-05)	AP2-14 (1.2E-04) E1-7 (1.7E-05) E4-6 (1.6E-06)	

Note. The number after the crew failure mode label indicates the crew failure scenario chosen on the crew failure mode decision tree (e.g., AP2-14 corresponds to crew failure scenario 14 on the decision tree for Crew Failure Mode AP2). Refer to Appendix B for a complete list of the crew failure mode decision trees and human error probabilities associated with the crew failure scenarios on each crew failure mode decision tree. Crew failure modes in bold indicate that the crew failure mode was a main contributor to the final human error probability.

All the teams generally agreed on the procedural path, the cues for diagnosing total loss of feedwater, and what the operators need to do in response to a total loss of feedwater. Similar to Human Failure Event 1, the differences in the teams' task analyses were driven by task decomposition and execution task modeling.

- Although Team 1 and 5 recognized that the operators would need to transfer to ES-01 from E-0 and monitor critical safety function status trees, they expected the task to be an assumed success, and therefore did not quantify the task.

- Team 4 decomposed the execution of feed and bleed (Critical Task 3) into two subtasks, which is not consistent with IDHEAS AT-POWER guidance for treating execution tasks holistically.

- Unlike other teams, Team 5 modeled the transfer from Step 2 to Step 10 in FRH-1 as a critical task in their crew response diagram.

- Team 2 and 3 categorized Critical Task 3 as complex whereas Team 1 and 5 treated it as simple.

3.3.2.3 Recovery Modeling

Teams 1, 3, and 5 identified a recovery path for each critical task. In contrast, Teams 2 and 4 only identified recovery for some of the critical tasks and did not document the rationale for why some critical tasks did not have recovery.

3.3.2.4 Assessment of Crew Failure Modes and Performance-Influencing Factors

The five teams' assessment of crew failure modes and performance-influencing factors for Human Failure Event 2 is summarized in Table 3-2~~Table 3-2~~.

3.3.2.4.1 Critical Task 1: Enter ES-01 and Monitor Critical Safety Function Status Trees

Teams 1 and 5 did not quantify Critical Task 1 because they expected this task to be a success due to operator training. The other teams estimated low failure probabilities for this task, suggesting agreement among the teams in terms of their understanding of the scenario.

The differences observed in decision tree path selection for Team 2, 3, and 4 reflected different opinions on recovery and workload level. Teams 2 and 4 did not identify recovery potential for this task, whereas Team 3 identified the potential for recovery in subsequent steps of the procedure. Similar to their analysis for Human Failure Event 1, Team 4 rated the workload performance-influencing factor as high for Crew Failure Mode SA3 (Critical Data Misperceived) and low for Crew Failure Mode AP2 (Misread or Skip Step in Procedure). Team 3 believed that workload would be low for SA3.

3.3.2.4.2 Critical Task 2: Identify Total Loss of Feedwater (TLOFW) and Enter FRH-1

As discussed above, all the teams agreed that Crew Failure Mode SA1 (Data Misleading or Not Available) was the dominating failure mode for Human Failure Event 2, but they disagreed on the performance-influencing factors for Distraction, Guidance to Seek Confirmatory Data, and Information Obviously Incorrect. The disagreement on Information Obviously Incorrect was caused by the fact that one team evaluated a different primary cue. Teams 1, 2, 3, and 5

evaluated the auxiliary feedwater flow indication, whereas Team 4 referred to the steam generator level as the primary cue. Other teams characterized the steam generator level as an alternative cue to confirm the auxiliary feedwater flow. Unlike other teams, Teams 2 and 5 argued that Distraction was low because there were no other competing tasks. Team 1 noted that they were not sure whether to rate Distraction as high or low based on the guidance. Although Team 1 ended up choosing high Distraction for Crew Failure Mode SA1, they chose low workload for Crew Failure Mode AP2 (Misread or Skip Step in Procedure).

The teams chose most of the same crew failure modes (e.g., Crew Failure Mode AP2 (Misread or Skip Step in Procedure), SA3 (Critical Data Misperceived), and RP2 (Choose Inappropriate Strategy)), but different crew failure scenarios within those crew failure modes, which indicates their disagreement on the performance-influencing factors for workload, training, and recovery potential. However, these differences did not have a significant effect on the final human error probabilities because the failure probabilities for Crew Failure Mode SA1 were so much higher than the probabilities for other crew failure modes. Although Team 2 had a recovery path for Critical Task 2 in their crew response diagram, they did not always credit recovery potential for the crew failure modes they selected (e.g., AP2-13 (Misread or Skip Step in Procedure), SA3-15 (Critical Data Misperceived)).

Unlike other teams, Team 3 selected Crew Failure Mode SA4 (Critical Data Dismissed/Discounted) and SA5 (Premature Termination of Critical Data Collection) as possible crew failure modes for Critical Task 2. This seems to be a result of the team's interpretation of the scope of the crew failure modes, which was not consistent with the guidance as intended. Misinterpretation of the guidance may also explain why Team 4 selected Crew Failure Mode RP2 (Choose Inappropriate Strategy).

3.3.2.4.3 Critical Task 3: Implement Feed and Bleed

There was significant variability in the crew failure modes chosen for Critical Task 3. Team 1, 4, and 5 treated Task 3 as a simple execution, whereas Teams 2 and 3 treated it as a complex execution, which is inappropriate in this case. The difference resulted in failure probabilities that were different by one order of magnitude. In addition, Teams 2, 3, and 5 inappropriately selected nonexecution crew failure modes (e.g., Crew Failure Mode AP-2) when feed and bleed should be considered a purely execution task.

Similar to Team 4's selection of Crew Failure Mode RP2 (Choose Inappropriate Strategy) for Critical Task 2, Team 2 appeared to misinterpret the scope of Crew Failure Mode RP2 and selected it as a crew failure mode for Critical Task 3.

Similar to Human Failure Event 1, most teams selected Crew Failure Mode E3 (Failure to Initiate Execution) and the lower-most crew failure scenario on the decision tree. However, this crew failure scenario has a high enough failure probability so that it dominates the teams' execution human error probabilities. Although the contribution of Crew Failure Mode SA1 (Data Misleading or Not Available) was the primary driver for each team's final human error probability, the contribution of the failure to execute could have been more significant if the scenario did not include a misleading indicator.

3.3.3 Human Failure Event 3

3.3.3.1 Estimated vs. Expected Human Error Probabilities

The estimated human error probabilities for Human Failure Event 3 were very similar to the teams' expected human error probabilities (Figure 3-7~~Figure 3-7~~). In addition, the estimated human error probabilities fell within a narrower range (2.3E-01 to 2.6E-02) than the expected human error probabilities (5E-01 to 7E-03). Compared to other teams, the expected human error probabilities of Teams 3 and 4 deviated more from their estimated human error probabilities. One result that is worth noting was that Teams 2 and 4 obtained the same human error probabilities with the selection of the same set of crew failure modes and decision tree paths. Team 1's relatively higher human error probability was primarily caused by their use of Crew Failure Mode SA1 (Data Misleading or Not Available); it was not used by other teams because the data required by the procedures was available and correct—it was the procedures that were deficient, not the data. Without using this crew failure mode, Team 1's human error probability would have been closer to those of other teams.

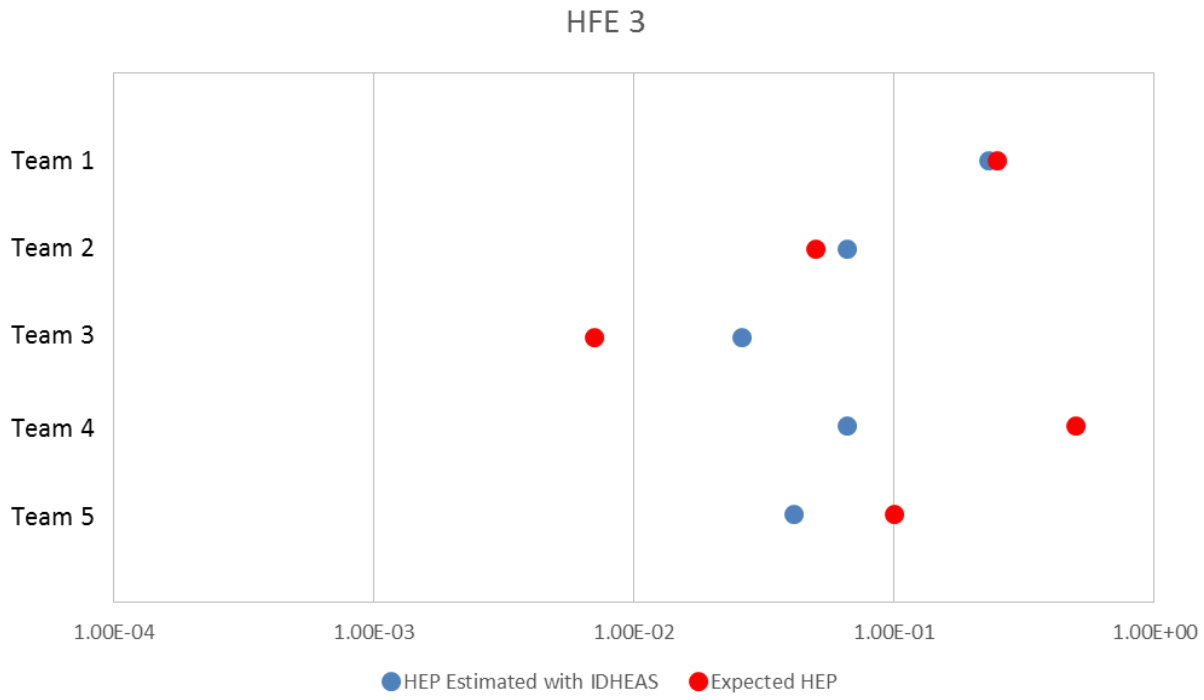


Figure 3-7 Comparison of Estimated and Expected Human Error Probabilities for Human Failure Event 3

Although the estimated human error probabilities were all within one order of magnitude of each other, the teams derived those human error probabilities using different crew failure modes as the dominating contributor to the failure probability. Team 2 and 4 used Crew Failure Mode AP1 (Key Alarm Not Attended To) as the dominating failure mode. Team 1 also used Crew Failure Mode AP1, but their final human error probability was dominated by their use of Crew Failure Mode SA1 (Data Misleading or Not Available). Team 5's final human error probability was dominated by Crew Failure Mode RP1 (Misinterpret Procedure). Team 3 was the only team to

use an execution crew failure mode as the dominant failure mode (i.e., Crew Failure Mode E3 (Failure to Initiate Execution)). The relatively larger contribution of the execution crew failure mode to Team 3's final human error probability can be explained by their conclusion that the operators would delay opening FCV-626 due to other competing tasks.

3.3.3.2 Critical Tasks and Procedural Paths

The five teams identified some or all of the following critical tasks (see Table 3-3).

- Critical Task 1: Identify loss of seal cooling
    - Detect APP-001-D1 alarm and enter APP-001-D1 alarm response procedure (Teams 1, 3, 4, and 5).
    - Enter AOP-018 Section C upon reactor coolant pump alarms (Team 2).
- Critical Task 2: Verify elapsed time since loss of seal cooling (Only Teams 1 and 5 explicitly modeled this task).
- Critical Task 3: Open FCV-626
    - Open FCV-626 in APP-001-D1 (Teams 1, 3, and 4).
    - Open FCV-626 in AOP-018 (Teams 2 and 5).

Both APP-001-D1 alarm response procedure and AOP-018 Section C provide guidance to open FCV-626. The teams identified different procedural paths and critical tasks due to the differences in their assumptions regarding the following aspects of the scenario:

- Teams 1, 3, 4, and 5 expected the operators to enter APP-001-D1 alarm response procedure upon APP-001-D1 alarm, which will be annunciated at the beginning of the scenario. In contrast, Team 2 expected AOP-018 Section C to be entered upon reactor coolant pump alarms after CVC-310A fails open, which occurs 44 minutes into the scenario. Note that although Team 4 recognized that FCV-626 could be opened in AOP-018, they believed that the operators were not likely to transition to AOP-018.
- Although Teams 1, 3, 4 and 5 expected entry of APP-001-D1, they disagreed on how the procedure would be entered. Teams 1, 3 and 4 expected the operators to be aware of the importance of the APP-001-D1 alarm and respond to the alarm sometime, if not immediately, after it was detected, whereas Team 5 expected the operators to attend to the alarm response procedure through a directed search per procedural guidance in Path-1. Team 5 considered that even if the alarm were detected early in the sequence, it would not have been given priority. As discussed below, this difference caused differences in recovery modeling.
- APP-001-D1 alarm response procedure instructs operators to check seal injection flow rate before opening FCV-626. The flow rate should be below 6 gpm in this scenario, which implies loss of seal injection. However, the procedure does not specify what to do if the flow rate is low. Teams 1 and 4 assumed that the operators would go to the next step to open FCV-626 regardless of the flow rate, whereas Team 5 assumed that the operators would transition to AOP-018 upon detection of loss of seal injection rather than

immediately open the valve in APP-001-D1. Team 3 seemed to recognize the unclear nature of the procedure and tried to use Crew Failure Mode RP1 (Misinterpret Procedure) to capture the potential failure, which was not within the intended scope of the crew failure mode.

- The flow control valve (FCV-626) should not be opened if reactor coolant pump seal cooling has been lost for more than 15 minutes due to risk of seal damage. This requirement is specified in AOP-018, but not APP-001-D1. Although Team 1 did not expect that AOP-018 would be entered, they conservatively assumed this requirement and explicitly modeled it as a critical task (i.e., Critical Task 2). Team 2 acknowledged the requirement but did not model it as a critical task. Instead, the team documented their assumption that the elapsed time from loss of seal cooling was less than 15 minutes. Team 5 concluded that the elapsed time was less than 15 minutes based on a timing analysis. Other teams did not explicitly consider this timing requirement.

3.3.3.3 Recovery Modeling

Differences in the primary cues used to identify total loss of seal cooling led to differences in the cues used in recovery modeling. Team 5 used reactor coolant pump alarms as recovery cues for the detection of loss of all seal cooling, which were primary cues in Team 2's analysis. Team 3 used Path-1 as a recovery cue, which was the primary cue in Team 5's analysis. Team 1 used both reactor coolant pump alarms and Path-1 as recovery cues. In contrast, Team 4 did not model any recovery potentials.

In Team 3's analysis, Critical Tasks 1 and 3 were grouped together with a recovery path. The recovery path is misleading in that it suggests that it would recover the failure of both identifying the loss of seal cooling and opening FCV-626. However, the recovery, which is identified as a directed check of the D1 alarm in the procedures, only recovers the failure to identify loss of seal cooling. Team 3 incorrectly credited recovery for the execution crew failure modes for opening FCV-626 (i.e., Crew Failure Mode E3-2 and E4-6). The method guidance directs analysts to credit recovery potential on a decision tree if a recovery path is identified for a corresponding critical task. Team 3 followed the guidance verbatim and credited recovery for all crew failure modes identified as applicable to their broadly defined critical task. This suggests that the team may have misunderstood the intent of the guidance.

3.3.3.4 Assessment of Crew Failure Modes and Performance-Influencing Factors

The five teams' assessment of crew failure modes and performance-influencing factors for Human Failure Event 3 is summarized in Table 3-3.

3.3.3.4.1 Critical Task 1: Identify Loss of Seal Cooling

Since the teams expected the operators to identify loss of seal cooling in different ways with different cues, they identified different failure modes for Critical Task 1. Teams 1, 2, 3, and 4 expected the operators to detect the loss of seal cooling cues through alarm response. As a result, they identified Crew Failure Mode AP1 (Key Alarm Not Attended to) as the potential failure mode. This crew failure mode is not applicable to directed alarm search, which is how Team 5 modeled loss of all seal cooling identification.

Table 3-3 Comparison of Teams' Analysis for Human Failure Event 3

HFE 3: Loss of RCP Seal Cooling – Restore Cooling from CCW by Opening FCV-626						
Team		*Critical Tasks*				*HEP*
		Identify Loss of Seal Cooling		**Verify Elapsed Time (< 15 min)**	**Open FCV-626**	
1	**Analysis**	Crew responds to D1 alarm after plant is stabilized. Path-1, B11 and RCP alarms modeled as recovery.		Verification of elapsed time is conservatively assumed.		**2.3E-01**
	CFMs	AP1-3 (6.5E-02) **SA1-4 (1.5E-01)**		SA3-3 (1.1E-02)	AP2-13 (8.2E-04) E3-5 (1.4E-04) E4-7 (9.3E-06)	
2	**Analysis**	Crew enters AOP-018 Section C upon various cues after CVC-310A fails open rather than APP-001-D1.		Verification of elapsed time is acknowledged but not modeled as a critical task. Assumes elapsed time is less than 15 minutes.		**6.6E-02**
	CFMs	**AP1-3 (6.5E-02)**			A2-7 (1.0E-03) E3-5 (1.4E-04) E4-5 (9.3E-06)	
3	**Analysis**	Crew detects D1 alarm. Path-1, B11 modeled as recovery. RCP alarms not considered.		Not modeled.	Modeled as part of critical task 1.	**2.6E-02**
	CFMs	AP1-4 (4.4E-03) SA2-12 (3.2E-04) RP1-4 (5.3E-03) E1-7 (1.7E-05) **E3-2 (1.6E-02)** E4-6 (1.6E-06)				
4	**Analysis**	Crew detects D1 alarm. Path-1 B11 considered but not modeled as recovery. RCP alarms not considered.		Not modeled.		**6.6E-02**
	CFMs	**AP1-3 (6.5E-02)**			AP2-7 (1.0E-03) E3-5 (1.4E-04) E4-5 (9.3E-06)	
5	**Analysis**	Identification of loss of seal cooling from CCW. Crew responds to D1 alarm at Path-1 B11. RCP alarms modeled as recovery.	Identification of loss of seal injection. Crew enters AOP-018, Section C. RCP alarms modeled as recovery.	Addressed timing analysis.		**4.1E-02**
	CFMs	AP2-8 (1.5E-04) SA2-12 (3.2E-04) RP1-4 (5.3E-03)	AP2-8 (1.5E-04) SA3-10 (1.3E-04) **RP1-2 (3.3E-02)**	AP2-13 (8.2E-04) SA3-15 (1.3E-05)	AP2-13 (8.2E-04) E3-5 (1.4E-04) E4-7 (9.3E-06)	

Note. The number after the crew failure mode label indicates the crew failure scenario chosen on the crew failure mode decision tree (e.g., AP2-14 corresponds to crew failure scenario 14 on the decision tree for Crew Failure Mode AP2). Refer to Appendix B for a complete list of the crew failure mode decision trees and human error probabilities associated with the crew failure scenarios on each crew failure mode decision tree. Crew failure modes in bold indicate that the crew failure mode was a main contributor to the final human error probability.

3.3.3.4.2 Critical Task 2: Verify Elapsed Time since Loss of Seal Cooling

Although both Team 1 and Team 5 identified Crew Failure Mode SA-3 (Critical Data Misperceived), the teams disagreed on the performance-influencing factors of human system interface (HSI) and workload. Team 1 selected poor human system interface and high workload, whereas Team 5 selected good human system interface and low workload.

3.3.3.4.3 Critical Task 3: Open FCV-626

All teams identified Crew Failure Mode E3 (Failure to Initiate Execution) and Crew Failure Mode E4 (Failure to Correctly Execute Simple Response). Except for Team 3, most teams agreed that the operators would not be likely to fail to initiate execution. Team 3 concluded that there were other competing tasks so that the operators would delay opening FCV-626, which can be captured by Crew Failure Mode E1 (Delay Implementation). The fact that Team 3 selected both Crew Failure Modes E1 and E3 to double count the effect suggests that the team was not clear on the scope of the crew failure modes.

In addition, the teams did not agree on the performance-influencing factor of workload for Crew Failure Mode E4 (Failure to Correctly Execute Simple Response). Team 1 and 5 chose low workload for this performance-influencing factor, whereas Team 2, 3, and 4 chose high workload. However, the failure probabilities in the decision tree are the same (9.3E-06) regardless of whether workload is high or low, as long as the simple task has nominal human system interface and recovery potential (i.e., decision tree paths E4-5 or E4-7).

3.3.4 Human Failure Event 4

3.3.4.1 Estimated vs. Expected Human Error Probabilities

The estimated human error probabilities for Human Failure Event 4 are similar to the teams' expected human error probabilities and fall in a relatively narrow range (Figure 3-8~~Figure 3-8~~). All teams expected this human failure event to be moderately difficult, with expected human error probabilities ranging from 2E-01 to 3.3E-02. Team 4 had the greatest difference between the estimated and expected human error probability, but even that difference was only about one order of magnitude. Teams 3 and 4 produced approximately the same human error probability; however, the teams did not agree on the dominating crew failure modes. The failure probabilities for execution crew failure modes dominate Team 1 and Team 5's final human error probabilities, but the dominating crew failure modes are different. Team 2, 3, and 4's results are dominated by status assessment and response planning human error probabilities, but again the dominating failure modes and performance-influencing factors differ.

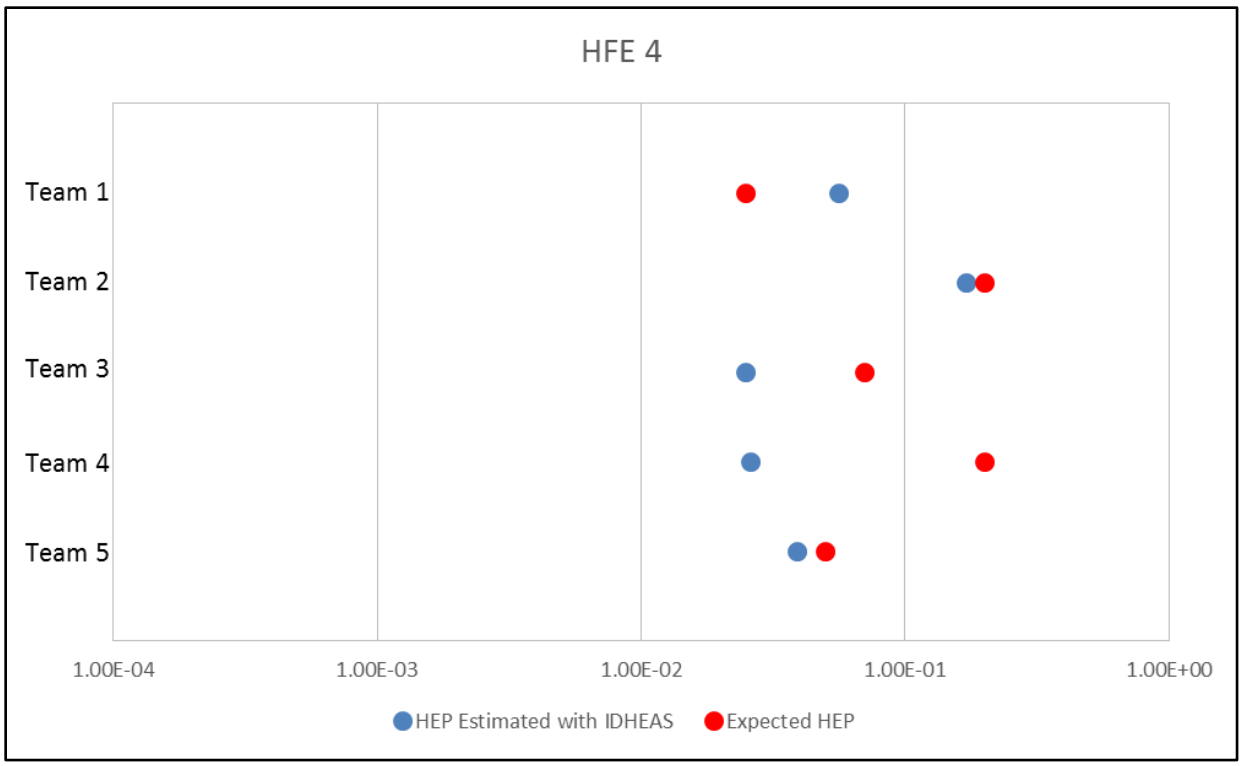


Figure 3-8 Comparison of Estimated and Expected Human Error Probabilities for Human Failure Event 4

3.3.4.2 Critical Tasks and Procedural Paths

The five teams identified some or all the following critical tasks (see

- Critical Task 1: Identify loss of seal injection and cooling and enter AOP-018, Section C
- Critical Task 2: Verify elapsed time since loss of seal cooling. (Only Teams 1 and 5 explicitly modeled this task.)
- Critical Task 3: Trip reactor coolant pumps

Although all teams identified Critical Task 1, the teams varied with regard to the primary cues and procedural paths used.

- Team 1 modeled Human Failure Event 4 as the continuous event evolution after Human Failure Event 3 with the boundary condition defined by the end state of Human Failure Event 3. Hence, the operators were assumed to be in APP-001-D1 for Human Failure Event 4.
- The boundary condition of Human Failure Event 4 was not clearly defined or documented in Team 2's analysis. It seems that the operators were assumed to be already in AOP-018 and then transfer to Step 3 based on the 15-minute timing requirement for restoring seal cooling.

- Team 3 modeled Human Failure Event 4 from the beginning of the scenario. The team expected the operators to identify loss of seal injection and cooling and then transition to AOP-018 when Path-1 B11 instructs the operators to check if at least one charging pump is running.

- Team 4 modeled Human Failure Event 4 from when CVC-310A fails fully open, which causes seal injection to be inadequate. The team expected the operators to identify loss of seal injection and cooling and then transition to APP-001-C2 and then to AOP-018 upon receiving Reactor Coolant Pump #1 SEAL LEAKOFF HI TEMP alarm, which occurs late in the scenario and only gives 5 minutes for operators to trip reactor coolant pumps. Note that while other teams considered transferring to Section C after entry of AOP-018 an assumed success, this task was modeled as a critical task and a dominating human error probability contributor in Team 4's analysis. Team 4 believed that given the short time window, failure to transfer to Section C after entry of AOP-018 would not give the operators enough time to recover. The team disagreed with other teams on whether the instruction on procedural transfer was clear.

- Similar to Team 3, Team 5 modeled Human Failure Event 4 from the beginning of the scenario. The team expected the operators to identify loss of seal injection and cooling and then transition to AOP-018 upon receiving Reactor Coolant Pump B High Bearing Temperature alarm.

3.3.4.3 Recovery Modeling

The discussion in the previous section suggests that reactor coolant pump alarms are legitimate cues for identification of loss of seal injection. They were considered by Team 3 as recovery but not by Team 1. Team 5 considered the first reactor coolant pump alarm (Reactor Coolant Pump B High Bearing Temperature alarm) as the primary cue and used other reactor coolant pump alarms for recovery.

3.3.4.4 Assessment of Crew Failure Modes and Performance-Influencing Factors

The five teams' assessment of crew failure modes and performance-influencing factors for Human Failure Event 4 is summarized in Table 3-4.

3.3.4.4.1 Critical Task 1: Identify loss of seal cooling

The teams agreed on high workload for Critical Task 1. The teams expected the operators to identify loss of seal injection in different ways with different cues, and thus they identified different failure modes for Critical Task 1. Teams 4 and 5 expected the operators to detect the loss of seal injection cues via alarms. As a result, they identified Crew Failure Mode AP1 (Key Alarm Not Attended To) as the potential failure mode. Note that Crew Failure Mode AP1 is not applicable to an indication search directed by procedure, which is how Teams 1 and 3 modeled the identification of loss of seal injection. However, Team 3 used Crew Failure Mode AP1, which was not consistent with the method guidance, given how they modeled Critical Task 1.

While other teams considered transferring to Section C after entry of AOP-018 an assumed success, this task was modeled as a critical task and a dominating human error probability contributor in Team 4's analysis.

3.3.4.4.2 Critical Task 2: Verify elapsed time since loss of seal cooling

While all teams considered the 15-minute time requirement for restoring seal cooling, only Teams 1 and 5 explicitly modeled it as a critical task. Both Team 1 and Team 5 selected Crew Failure Mode AP2 (Misread or Skip Step in Procedure) and Crew Failure Mode SA3 (Critical Data Misperceived) as failure modes for Critical Task 2. For Crew Failure Mode AP2, the teams disagreed on whether there were compensatory factors for continuous action procedural steps, which seems to be caused by their different opinions on work practices and training. Due to insufficient information, Team 5 assumed the compensatory factors to be present under the assumption of nominal work practice and training. In contrast, Team 1 believed that use of the continuous action steps relies on the operators to act when required, and it is not well covered by human performance techniques to aid operators in place keeping (e.g., circle/slash technique).

Evaluator commentary: The two teams treated Critical Task 2 as a nonexecution task. However, it is arguable whether Critical Task 2 can be treated as an execution task. The operators should be aware of seal injection after they enter AOP-018. What they are doing is to monitor time per a continuous procedural step while trying to restore seal cooling. There is no important status assessment activity at this point. Team 5 selected Crew Failure Mode E2 (Critical Data Not Checked with Appropriate Frequency) to capture the potential failure in the monitoring task. It is not clear whether the use of Crew Failure Mode E2 is appropriate in this situation. This may be reflective of a gap in the method in capturing the potential failure modes of the monitoring activities in executing a continuous action procedural step, or more generally, insufficient guidance for modeling execution of continuous action procedural steps.

3.3.4.4.3 Critical Task 3: Trip Reactor Coolant Pumps

All teams selected Crew Failure Mode E3 (Failure to Initiate Execution) and Crew Failure Mode E4 (Failure to Correctly Execute Simple Task) for Critical Task 3. Team 1 and Team 3 also selected Crew Failure Mode E1 (Delay Implementation) because restoring cooling to the reactor coolant pump seals would be preferable to tripping reactor coolant pumps and isolating without cooling. However, the two teams disagreed on whether the operators had a correct assessment of operational margin so that the operators thought they could delay implementation longer than they could.

The teams also disagreed on whether workload was high or low when assessing the crew failure modes for Critical Task 3. Team 5 chose low workload for Crew Failure Mode AP2 (Misread or Skip Step in Procedure), whereas the other teams chose high workload. As in Human Failure Event 3, Team 1 and 5 chose low workload for Crew Failure Mode E4 (Failure to Correctly Execute Simple Task), whereas Team 2, 3, and 4 chose high workload. However, because the probabilities for crew failure scenario E4-5 and E4-7 are the same, this difference did not impact the final human error probabilities.

Table 3-4 Comparison of Teams' Analysis for Human Failure Event 4

HFE 4: Loss of RCP Seal Cooling – Trip RCPs to Avoid Seal Failure							
Team		*Critical Tasks*					*HEP*
		Identify Loss of Seal Injection and Cooling, Enter AOP-018			**Verify Elapsed Time**	**Trip RCPs**	
1	**Analysis**	Crew assumed to be in D1. Enter AOP-018 upon low seal injection flow. RCP alarms not considered for recovery. Transfer to Section C assumed success.			Continuous action step.	Delay implementation possible because restoring cooling to RCP seals preferred.	**5.6E-02**
	CFMs	AP2-7 (1.0E-03) SA2-11 (2.0E-03) SA3-11 (1.6E-04) SA4-16 (N/A)			AP2-5 (1.3E-02) SA3-11 (1.6E-04)	AP2-7 (1.0E-03) **E1-3 (3.8E-02)** E3-5 (1.4E-04) E4-7 (9.3E-06)	
2	**Analysis**	Unclear how crew enters AOP-018. Transfer to Section C not explicitly modeled.			Assessment of time is acknowledged and not modeled as a critical task.		**1.7E-01**
	CFMs	**AP2-1 (9.4E-02)** SA3-11 (1.6E-04) **RP1-3 (7.3E-02)**				AP2-7 (1.0E-03) E3-5 (1.4E-04) E4-5 (9.3E-06)	
3	**Analysis**	Assume crew will check seal injection flow at Path-1, C10. RCP alarms modeled as recovery. Transfer to Section C assumed success.			Assessment of time is acknowledged and not modeled as a critical task.	Delay implementation possible because restoring cooling to RCP seals preferred.	**2.5E-02**
	CFMs	**AP1-4 (4.4E-3)** AP2-4 (2.7E-3) SA2-12 (3.2E-4) SA3-12 (3.4E-5) **RP1-4 (5.3E-3)**				AP2-7 (1.0E-03) **E1-2 (1.1E-02)** E3-5 (1.4E-04) E4-5 (9.3E-06)	
4	**Analysis**	Respond to alarm C2: RCP #1 seal leakoff high temp. Assume 5 minutes available to trip RCPs.	Enter AOP-018 upon #1 seal failure.	Transfer to Section C based on RCP alarms.	Assessment of time is acknowledged and not modeled as a critical task.		**2.6E-02**
	CFMs	AP1-4 (4.4E-03)	AP2-7 (1.0E-03) RP1-8 (N/A)	**AP2-3 (1.9E-02)** RP1-8 (N/A)		AP2-7 (1.0E-03) E3-5 (1.4E-04) E4-5 (9.3E-06)	
5	**Analysis**	Enter AOP-018 upon low seal injection flow. RCP alarms modeled as recovery. Transfer to Section C assumed success.			Continuous action step.	Low workload.	**3.9E-02**
	CFMs	AP1-4 (4.4E-03) SA4-16 (N/A)			AP2-7 (1.0E-03) SA3-11 (1.6E-04) **E2-3 (3.2E-02)**	AP2-13 (8.2E-04) E3-5 (1.4E-04) E4-7 (9.3E-06)	

Note. The number after the crew failure mode label indicates the crew failure scenario chosen on the crew failure mode decision tree (e.g., AP2-14 corresponds to crew failure scenario 14 on the decision tree for Crew Failure Mode AP2). Refer to Appendix B for a complete list of the crew failure mode decision trees and human error probabilities associated with the crew failure scenarios on each crew failure mode decision tree. Crew failure modes in bold indicate that the crew failure mode was a main contributor to the final human error probability.

3.3.5 Human Failure Event 5

3.3.5.1 Estimated vs. Expected Human Error Probabilities

The teams' estimated human error probabilities significantly deviated from each other, leading to approximately three orders of magnitude difference, which echoes the disagreement of the teams in the expected human error probabilities of the human failure event (Figure 3-9~~Figure 3-9~~). Nonetheless, each team's estimated human error probability is fairly consistent with their expected human error probability. Team 1 had the greatest difference between their estimated and expected human error probability, but that difference was still within one order of magnitude. Team 1 may have had a slightly higher estimated human error probability had they quantified Critical Tasks 1 and 2, which may have made their final human error probability more consistent with the expected human error probability.

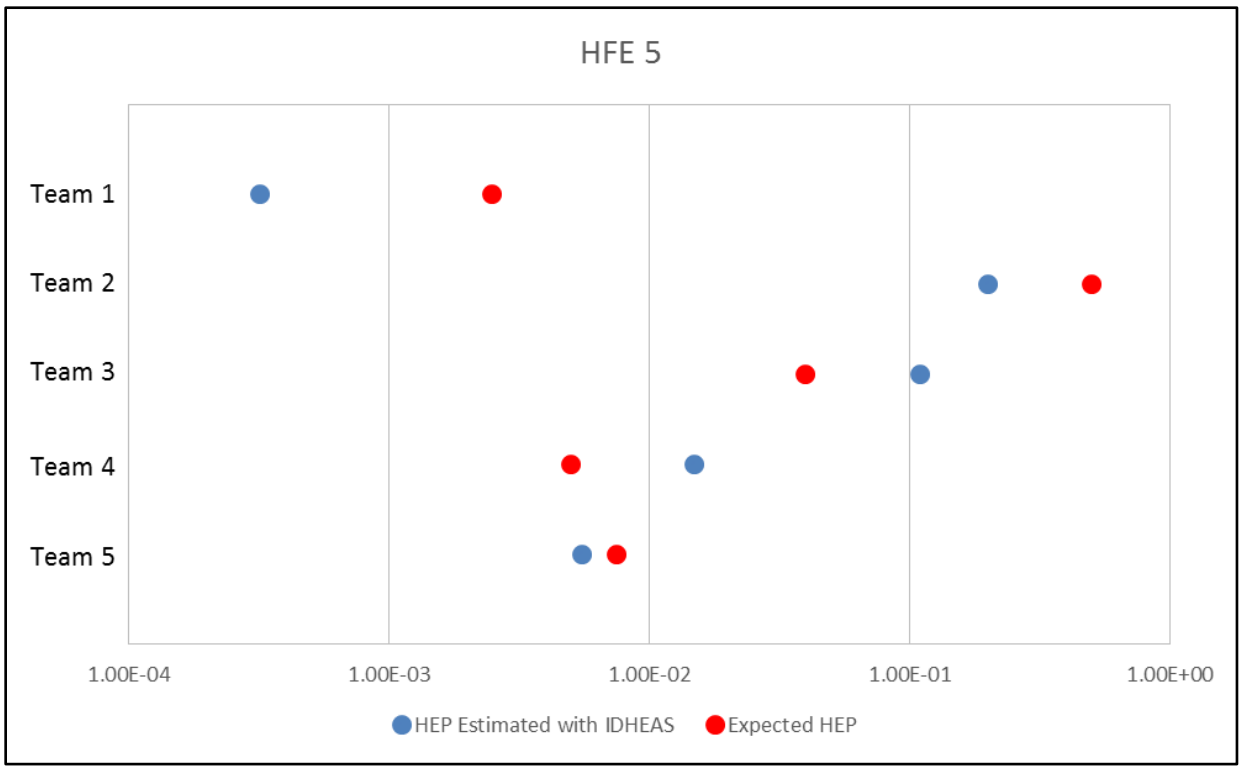


Figure 3-9 Comparison of Estimated and Expected Human Error Probabilities for Human Failure Event 5

3.3.5.2 Critical Tasks and Procedural Paths

The five teams identified some or all the following critical tasks (see Table 3-5).

- Critical Task 1: Diagnose small loss-of-coolant accident
- Critical Task 2: Transfer to EPP-8
- Critical Task 3: Cooldown and depressurize reactor coolant system

The five teams generally agreed on the procedural paths and associated cues for diagnosing the small loss-of-coolant accident and making procedural transfers. The consistency can be attributed to the timing and thermohydraulic information given to the analyst teams by the designated operator. Nonetheless, the teams varied in the following aspects.

Although all teams agreed on Critical Tasks 1 and 2, Team 1 believed that the two tasks were very unlikely to fail and did not quantify the tasks. Team 4 chose to combine the two tasks as one. Unlike other teams, Team 2 broke down Critical Task 3 into four simple execution tasks. The other teams modeled the reactor coolant system cooldown and depressurization as a single task.

3.3.5.3 Recovery Modeling

Team 5 identified recovery paths for Critical Tasks 1 and 2 based on interviews with the designated operator. Team 1 identified recovery paths for all three critical tasks based on interviews with the designated operator as well; however, since Critical Task 3 is treated as a complex control action, similar to the cooldown and depressurization task in Human Failure Event 1, recovery modeling is not necessary because it cannot be credited within the decision tree for the complex execution crew failure mode. Teams 2 and 4 did not identify any recovery paths in their analysis of Human Failure Event 5 because they believed that although the response was feasible, there was not adequate time for recovery. Team 3 did not identify a recovery path on their crew response diagram, but they credited recovery for Critical Task 1 because procedure Path-1 provided multiple steps to identify small loss-of-coolant accident; however, they did not provide justification why there was no recovery for other critical tasks.

The differences in recovery modeling were partly caused by the different interpretations of the time window of Human Failure Event 5. Team 1 seemed to interpret the time window as the time available to reach Step 29 of EPP8, which was considered consistent with how the time window was defined in the human failure event (i.e., time available to initiate cooldown and depressurization). In contrast, other teams interpreted the time window to be the time taken to cool down the plant below 400°F because the designated operator indicated that was the implicit criterion for successful operator response to the small loss of coolant accident as defined in Human Failure Event 5.

3.3.5.4 Assessment of Crew Failure Modes and Performance-Influencing Factors

The five teams' assessment of crew failure modes and performance-influencing factors for Human Failure Event 5 is summarized in Table 3-5.

Table 3-5 Comparison of Teams' Analysis for Human Failure Event 5

HFE 5: Loss of Seal Cooling – Depressurize RCS during SLOCA								
Team		*Critical Tasks*						*HEP*
		Diagnose SLOCA	**Transfer to EPP-8**	**Cooldown and Depressurize RCS**				
1	**Analysis**	Not quantified due to low failure likelihood.	Not quantified due to low failure likelihood.	Complex control action. Recovery not credited but considered.				**3.2E-04**
	CFMs			AP2-12 (9.7E-05) **E3-5 (1.4E-04)** E5-15 (8.0E-05)				
2	**Analysis**	Complex procedure. Inadequate time for recovery.	Complex procedure.	Cooldown.	Depressurize.	Minimize leakage.	Shutdown cooling.	**2.0E-01**
	CFMs	**AP2-1 (9.4E-02)**	**AP2-1 (9.4E-02)**	AP2-7 (1.0E-03) E2-11 (2.3E-03) E4-5 (9.3E-06)	AP2-13 (8.2E-04) E4-7 (9.3E-06)	AP2-13 (8.2E-04) E4-7 (9.3E-06)	AP2-7 (1.0E-03) E2-11 (2.3E-03) E4-7 (9.3E-06)	
3	**Analysis**	Recovery available. Procedure open to misinterpretation.		Complex control action.				**1.1E-01**
	CFMs	SA2-12 (3.2E-04) SA3-12 (3.4E-05) RP1-4 (5.3E-03)	AP2-7 (1.0E-03) SA3-12 (3.4E-05)	**AP2-3 (1.9E-02)** SA2-11 (2.0E-03) SA3-11 (1.6E-04) **RP1-3 (7.3E-02)** E1-6 (2.2E-04) E5-7 (3.8E-03)				
4	**Analysis**	Crew assumed to be in procedure Path-1. Diagnose SLOCA and transfer to EPP-8 modeled together. Inadequate time for recovery.		Complex control action. Poor work practices.				**1.5E-02**
	CFMs	AP2-7 (1.0E-03) SA3-11 (1.6E-04)		AP2-7 (1.0E-03) SA3-11 (1.6E-04) E1-6 (2.2E-04) E2-11 (2.3E-03) E3-5 (1.4E-04) **E5-5 (9.6E-03)**				
5	**Analysis**	Crew assumed to be in procedure Path-1. Recovery available.	Low workload.	Complex control action.				**5.5E-03**
	CFMs	AP2-8 (1.5E-04) SA2-12 (3.2E-04) SA3-12 (3.4E-05)	AP2-14 (1.2E-04) SA2-16 (5.2E-05) SA3-16 (1.3E-05)	AP2-13 (8.2E-04) E3-5 (1.4E-04) **E5-7 (3.8E-03)**				

Note. The number after the crew failure mode label indicates the crew failure scenario chosen on the crew failure mode decision tree (e.g., AP2-14 corresponds to crew failure scenario 14 on the decision tree for Crew Failure Mode AP2). Refer to Appendix B for a complete list of the crew failure mode decision trees and human error probabilities associated with the crew failure scenarios on each crew failure mode decision tree. Crew failure modes in bold indicate that the crew failure mode was a main contributor to the final human error probability.

3.3.5.4.1 Critical Task 1: Diagnose small loss-of-coolant accident and Critical Task 2: Transfer to EPP-8

Note that since Team 1 did not quantify Critical Tasks 1 and 2, the discussion of crew failure modes and performance-influencing factor selections does not include Team 1.

There is some commonality across the teams in the selected crew failure modes for Critical Tasks 1 and 2.

- All teams selected Crew Failure Mode AP2 (Misread or Skip Step in Procedure), which dominated Team 2's final human error probability and was an important contributor to the final human error probabilities of Teams 3, 4, and 5.

- Except Team 2, all other teams selected Crew Failure Mode SA2 (Wrong Data Source Attended To) or Crew Failure Mode SA3 (Critical Data Misperceived).

Much of the variability in the teams' human error probabilities can be attributed to teams' disagreement on ratings of the following performance-influencing factors for Critical Tasks 1 and 2.

- Procedure (complex or simple). Team 2 argued that Path-1 is complex because the procedure has multiple questions and multiple choices to make. This is one of the reasons that Team 2 chose crew failure scenario AP2-1 for Critical Tasks 1 and 2, which has a relatively high failure probability (9.4E-02). The Crew Failure Mode AP2-1 dominated Team 2's final human error probability and caused it to be the highest of the five teams. The other teams assessed the procedure as simple, arguing that multiple questions and multiple choices do not necessarily make the procedure complicated to understand or follow.

- Workload (high or low). Unlike other teams, Team 5 rated workload for Critical Task 2 to be low. They argued that when the operators reach the point on Path-1 where the crew would transfer to EPP-8 (Section I-12), the distraction has died down and the crew is focused only on Path-1. If the team had rated workload to be high and kept other performance-influencing factors the same, it would not have significantly increased the team's human error probability.

- Recovery potential (yes or no). Teams 3 and 5 credited multiple procedural steps to identify small loss-of-coolant accident for recovery, whereas Teams 2 and 4 did not credit recovery because they did not think there was adequate time for recovery.

- Procedure open to misinterpretation (yes or no). Team 3 argued that Path-1 is open to misinterpretation because the procedure does not indicate what normal indications are for small loss-of-coolant accident diagnosis. This caused the team to choose Crew Failure Mode RP1 (Misinterpret Procedures) in Critical Task 1. The team's rationale for PR1 is questionable as lack of normal indications does not necessarily make procedure ambiguous or complicated.

3.3.5.4.2 Critical Task 3: Cooldown and Depressurize Reactor Coolant System

All teams except Team 2 modeled Critical Task 3 as a complex control execution task and selected Crew Failure Mode E5 (Failure to Correctly Execute Complex Task); however, they disagreed on whether execution is straightforward or not, and whether work practices are good or poor. Team 1 believed that execution would be straightforward and chose crew failure scenario E5-15. Team 3, 4, and 5 believed the execution would not be straightforward, and therefore chose one of the higher decision tree paths for Crew Failure Mode E5. Team 4 chose failure scenario E5-5 because they believed that work practices would be poor and argued that the procedure required several continuous actions steps without further prompting to ensure key parameters are maintained. In contrast, both Team 3 and 5 assessed work practices as good and chose failure scenario E5-7. The disagreement caused Team 1's failure probability yielded from Crew Failure Mode E5 to be about two orders of magnitude smaller than those of other teams. The source of the disagreement seemed to be analysts' interpretation of the guidance for determining performance-influencing factor levels.

Teams 3 and 4 selected crew failure modes that fall in the phases of situational assessment and response planning for Critical Task 3. Note that Crew Failure Mode RP1 (Misinterpret Procedures) is the most dominating contributor to Team 3's final human error probability and causes the team's human error probability to be significantly higher than those of Teams 1, 4, and 5. Selection of nonexecution crew failure modes suggests that the analysts recognized that the complex execution task was not purely execution because it also involves cognitive activities. However, the practice of using nonexecution crew failure modes to address the cognitive activities involved in carrying out a complex execution is not consistent with the method guidance for modeling complex execution tasks.

The rationales for Team 3 to select Crew Failure Mode E1 (Delay Implementation) and Crew Failure Mode E2 (Critical Data Not Checked with Appropriate Frequency) and Team 4 to select Crew Failure Mode E2 are not clearly documented. Nonetheless, most performance-influencing factors associated with these crew failure modes were rated nominal, and the failure probabilities yielded from the crew failure modes were not large enough to significantly impact the final human error probabilities.

Teams 1, 4, and 5 selected Crew Failure Mode E3 (Failure to Initiate Execution) for Critical Task 3, but all agreed that this crew failure mode could be screened out because the teams selected the lowest decision tree path (E3-5), which is a screening path. Team 1's analysis indicates that they expected the complex control action of cooling down and depressurizing the reactor coolant system to be the main contributor to the human failure event, which suggests that Crew Failure Mode E-5 (Failure to Correctly Execute Complex Response) should drive their final human error probability. However, the failure probability associated with E3-5 (1.4E-04) is about twice as large as the failure probability yielded from Team 1's selection of E5-15 (8.0E-05), which therefore dominates their final human error probability. Although Team 1's human error probability is still very low, it may warrant additional consideration as to whether screening paths on the crew failure mode decision trees should be included in the calculation of the final human error probability.

3.4 Feedback from HRA Analysts

3.4.1 Method Usability

As part of the post-analysis questionnaire, the analyst teams were asked to rate, on a seven-point scale, how easy IDHEAS AT-POWER was to learn and use, and to what extent the guidance was clear. Their responses are listed in Table 3-6~~Table 3-6~~.

Table 3-6 Team Ratings of Usability of IDHEAS AT-POWER

	TEAM 1	TEAM 2	TEAM 3	TEAM 4
Easy to learn?	VERY DIFFICULT (6)	SOMEWHAT DIFFICULT (5)	SOMEWHAT EASY (3)	SOMEWHAT DIFFICULT (5)
Easy to use?	VERY DIFFICULT (6)	SOMEWHAT DIFFICULT (5)	SOMEWHAT DIFFICULT (5)	ABOUT AVERAGE (4)
Guidance clear?	SOMEWHAT UNCLEAR (5)	NEITHER CLEAR NOR UNCLEAR (4)	SOMEWHAT CLEAR (3)	SOMEWHAT CLEAR (3)

Regarding how easy IDHEAS AT-POWER was to learn, the ratings varied from Somewhat Easy (3) to Very Difficult (6). The teams indicated that there was a lot of information presented at the training workshop, and the process for using the method seemed relatively complicated. However, all the teams were able to use the training materials and guidance documents to successfully apply the method to the human failure events in the testing. All the teams chose to use the template provided by the testing team for documenting their results, which seemed to help the teams follow the steps of the IDHEAS AT-POWER guidance. However, some teams may have over-relied on the documentation template as a guide for conducting the analysis, instead of referencing back to the guidance in the IDHEAS AT-POWER report. This suggests that the framework used for documenting results can have a significant impact on how analysts use the method.

In terms of ease of use, the teams rated IDHEAS AT-POWER from About Average (4) to Very Difficult (6). On average, the teams thought the method was somewhat difficult to use. Teams noted the substantial documentation required to build the crew response diagram, and reliance on operator interviews to evaluate the crew failure modes and performance-influencing factors as contributing to the difficulty of the method. On the other hand, in terms of the utility of the method, the teams noted that the IDHEAS AT-POWER process forces analysts to develop a narrative of the human failure event. While it can be difficult and time consuming, it also results in a more thorough understanding of the failure mechanisms of the human failure event and the scenario as a whole. If used properly, IDHEAS AT-POWER has the capability to generate a detailed basis for each of the failure modes that contribute to the human failure event.

The teams rated the IDHEAS AT-POWER guidance as Somewhat Clear (3) to Somewhat Unclear (5). Additional comments about the guidance suggest that the teams tended to use the middle of the response scale because some parts of the guidance were easy to follow, whereas other parts caused confusion. In particular, the teams suggested additional guidance and examples would be helpful for selecting crew failure modes and evaluating performance-influencing factors.

3.4.2 Analysis Time

The number of hours that each team spent performing the analysis of each human failure event is listed in Table 3-7~~Table 3-7~~. The table also indicates the number of hours averaged for each human failure event and team. Overall, the teams reported that it was somewhat time-consuming to develop a crew response diagram and document the analysis. Identifying applicable crew failure modes appeared to be challenging for beginners. In addition, the teams found the documentation to be particularly long and sometimes redundant. On average, it took most teams about 38 hours to analyze one human failure event. However, as a caveat, the analysts in the current study were using IDHEAS AT-POWER for the first time, so additional effort is expected due to the learning curve when using a new method. The last row of Table 3-7~~Table 3-7~~ is the projected amount of time each team believes would be needed to analyze a human failure event with IDHEAS AT-POWER after an analyst had experience with the method. Although the projected time is less than the time spent, it is still considered to be high. At the post-analysis workshop, the analyst teams indicated that, from their experience, they would estimate that using IDHEAS AT-POWER would take twice as much time as other HRA methods that NRC and industry currently use.

Table 3-7 Reported Time Spent Analyzing Each Human Failure Event

	TEAM 1	TEAM 2	TEAM 3	TEAM 4	AVERAGE
HFE 1	50 hours	37 hours	40 hours	30 hours	39.25
HFE 2	32 hours	70 hours	42 hours	25 hours	42.25
HFE 3	40 hours	28 hours*	40 hours	20 hours	32
HFE 4	40 hours	28 hours*	38 hours	25 hours	32.75
HFE 5	30 hours	28 hours*	37 hours	25 hours	30
AVERAGE	38.4	38.2	39.4	25	35.25
PROJECTED AVERAGE**	16 hours	16-24 hours	16-24 hours	20-40 hours	

***Team 2 reported 84 hours for all analysis associated with Scenario 3 (Human Failure Events 3-5), time divided equally among human failure events.

**Projected average is the average amount of time each team believes would be needed per analyst to analyze a human failure event with IDHEAS AT-POWER after an analyst had experience with the method.

During the post-analysis workshop, the analyst teams were asked to estimate the proportion of time they spent on crew response diagram development versus crew failure mode and performance-influencing factor assessment. All the teams indicated that they spent more than half of their time developing their crew response diagrams. Team 2 indicated they spent nearly 80 percent of their time on crew response diagram development, whereas Team 3 spent about 70 percent, and Team 1 and 4 spent about 60 percent of their time on the crew response diagram. The teams also believed that additional experience with the method would make the selection of crew failure modes easier, particularly once one developed a working knowledge of all 14 crew failure modes and their associated decision trees. Analysts may also become more proficient with developing the crew response diagram through repeated use of the method. All the teams agreed that a computerized version of the tool could substantially reduce the amount of time needed to perform an analysis with IDHEAS AT-POWER. A tool like EPRI's HRA Calculator [11] could simplify the process of developing the crew response diagram and reduce redundancy in the documentation.

3.4.3 Task Analysis and Crew Response Diagram Development

The teams indicated that the process of defining nodes in the crew response diagram contributed to a more detailed understanding of the scenario. However, it was also noted that the process was time consuming and required near-expert understanding (e.g., licensed operator) of the procedures and plant. Analysts noted that the method's requirement to assess the entire procedure path is unlike other methodologies they have encountered. In other methodologies, it is necessary to validate that a procedure path exists, but not to evaluate it in any significant detail. The industry analysts thought it would be challenging to maintain consistency between human failure events that share common procedure paths, especially if different analysts assess the different actions in the same PRA model.

The teams thought more guidance was needed with regard to defining a crew response diagram node and critical task. The project team also noted that they encountered difficulty with providing a functional definition of a critical task in the training materials. One analyst noted that, even after the testing, they still had a difficult time describing what a critical task is, but they "know it when they see it." The teams struggled with determining whether operator actions should be modeled as one critical task or multiple critical tasks. The analysts noted that this could have an impact on the final human error probability because IDHEAS AT-POWER uses an additive approach. One team suggested that starting the analysis by grouping efforts into single nodes might increase efficiency and reduce the time required to analyze human failure events. Nodes could be separated into multiple critical tasks later if needed due to different cognitive activities or modeling of recoveries.

The analysts also commented that they had difficulty with modeling recovery. In terms of crew response diagram development, it was unclear how to depict recovery depending on the type of recovery. Some teams noted that they struggled with understanding how recoveries modeled in the crew response diagram should link to the recovery potential performance-influencing factors in the crew failure modes decision trees. Teams also indicated that searching for potential recoveries could be time intensive and require assessment of crew responses on a path that is not necessarily relevant or logical for plant conditions. One team suggested omitting the search for recovery paths if the resulting human error probability is reasonably low. If the human error probability is relatively high, then the time could be put into recovery path identification, application, and documentation.

The teams noted that the operator interviews were critical to the successful implementation of the method. One analyst described the interview process as being very different from other HRA methods, because of the need to develop a crew response diagram and answer questions about crew failure modes. They noted that the interview becomes more probing and iterative. Teams also noted that the method guidance helped them structure the interview and guided what questions they asked. Many of the analysts noted that detailed operational information was needed to perform the analysis, requiring a high level of knowledge and expertise on behalf of the HRA analyst or significant access to operators, training personnel, and the plant.

3.4.4 Assessment of Crew Failure Modes and Performance-Influencing Factors

The analyst teams strongly recommended additional guidance for choosing crew failure modes and assessing performance-influencing factors. Teams noted that the applicability criteria for some crew failure modes seemed too narrow, and additional examples in the crew failure mode selection guidance would be helpful. There were some crew failure modes that were almost always used by the analysts (e.g., Crew Failure Mode AP2, Crew Failure Mode SA3), whereas

other crew failure modes were rarely used (e.g., Crew Failure Mode RP2, Crew Failure Mode E2). Analysts were not always sure, based on the guidance, whether they were using the crew failure modes appropriately. Multiple teams suggested that more detail in the definitions of the crew failure modes would be helpful to make choosing the correct one easier. Another suggestion was made to include comparisons between similar crew failure modes and examples of the operator action they represent.

There was also confusion regarding the use of the guidance questions for assessing performance-influencing factors. The performance-influencing factor guidance questions were framed as "rules," suggesting that the questions were required as part of the performance-influencing factor assessment. However, analysts noted that some questions did not make sense, or the response criteria forced a performance-influencing factor assessment that did not appear to be appropriate. Analysts also found it odd that different crew failure modes had different questions for the same performance-influencing factor (e.g., workload), which may suggest that more clarification is needed on the performance-influencing factors. While this may be true, this difference was deliberate: since different aspects of a performance-influencing factor affect crew failure modes differently, the guidance questions were tailored for different crew failure modes when a performance-influencing factor appears in multiple crew failure modes.

Analysts also observed that some performance-influencing factor questions were unlikely to elicit a negative response. For example, operators and operations trainers are unlikely to ever answer decision tree branch point questions such as, "Is the crew trained on how to properly prioritize high workload situations?" (AP2, Branch Point 3 - Compensatory Factors) in the negative. One suggestion was to frame the performance-influencing factor guidance as examples rather than questions with an "if, then" framework. One team also observed that many of the examples in the guidance tended to be related to pressurized-water reactors; additional examples specific to boiling-water reactors would make the guidance more generally applicable to all U.S. power plants. Some teams also indicated that additional guidance was needed with regard to double-counting performance-influencing factors. One team expressed that it felt like they were double-counting, error-likely, performance-influencing factors in multiple crew failure modes, and they weren't sure whether that approach was correct.

All the teams thought that the workload performance-influencing factor would benefit from a more objective definition and examples to clarify high or nominal workload. In addition, the definition of simple or complex execution could be refined. One team suggested an additional execution category should be added for unusually complex actions (e.g., locally controlled equipment or electrical system actions with many subtasks).

3.4.5 Overall Feedback on Strengths and Weaknesses

The analyst teams agreed that the IDHEAS AT-POWER method facilitates a thorough assessment of operator response. The crew response diagram and timeline development necessitate a detailed understanding of the scenario. The process forces a narrative of the human failure event that can easily be bypassed when using other methods. If performed properly, the IDHEAS AT-POWER process will also generate a detailed basis for each of the contributors. This is especially true for recovery factors, which are typically not well documented or justified in other methodologies. Furthermore, IDHEAS AT-POWER encourages and relies upon qualitative assessments. Some degree of inconsistency between HRA analyses seems inevitable, but better consistency would be anticipated going forward, as analysts become more familiar with the method. There is a greater potential for in-depth review

by peers, which will also improve consistent application of the method. The process also requires the analyst to consider a multitude of questions, which might trigger identification of factors that the analyst may not have considered previously. Overall, the teams believed that the level of documentation and justification required of IDHEAS AT-POWER would lead to a more defensible HRA.

The teams noted that the IDHEAS AT-POWER process is still subjective, and therefore could be highly dependent on the analyst's interpretation of what factors are important to the human failure event when there is uncertainty about scenario dynamics. In addition, some teams thought the high level of operator involvement required to perform the operator interviews would be difficult to secure. All the teams agreed that IDHEAS AT-POWER was a time-intensive process. Some teams thought that it was much more difficult to use than the HRA Calculator [11] and SPAR-H [12] because of all the work in defining crew response diagram nodes and crew failure modes. However, the teams strongly believed that a software tool would help improve efficiency by reducing the need to document repetitive information and allowing for more organization and quick access to crew failure mode information. That being said, there was also some caution regarding the user interface of the software tool. A poorly designed tool could encourage analysts to take shortcuts and diminish the strengths of IDHEAS AT-POWER.

4 DISCUSSION

4.1 Validity

In general, IDHEAS AT-POWER appeared to have the capability to capture a broad range of failure modes, contextual conditions, and influences on behavior associated with the difficult human failure events and complex scenarios in the study. Its structured qualitative analysis framework encouraged a detailed assessment of timelines, procedures, and plant conditions. However, the thoroughness of the assessment was still somewhat dependent on analysts' HRA experience, human performance expertise, and operations knowledge. The set of crew failure modes and associated performance-influencing factors allowed analysts to identify failure causes at a fairly detailed level and translated qualitative analysis findings to assessing the human error probabilities in a coherent manner. In addition, the crew failure modes and performance-influencing factors seemed to have the ability to help analysts identify scenario vulnerability.

For Human Failure Events 1 and 2, the human error probabilities estimated with the method were not inconsistent with the simulator data and were within the range of other HRA methods' estimations in NUREG-2156, "The U.S. HRA Empirical Study." No team produced consistently optimistic or conservative human error probabilities. The differentiation in estimated human error probabilities across the human failure events varied across teams, ranging from one order of magnitude to three orders of magnitude. Similar observations were made for Human Failure Event 1 in the U.S. HRA Empirical Study; although the analyst teams in both this study and the U.S. HRA Empirical Study were familiar with the human failure event and agreed that operator response would be straightforward, the human error probabilities had variability of approximately two to three orders of magnitude. This echoed an observation from Kirwan [7] that HRA analysts have difficulty in accurately quantifying the lower end of the human error probability range.

4.2 Interanalyst Consistency

The study revealed some degree of variability among the teams' analyses, which was not consistent across the human failure events. As discussed in Section 3, there tended to be relatively less variability in the teams' qualitative analyses of human failure events associated with responses that are easy and familiar to analysts (e.g., Human Failure Event 1) and human failure events associated with responses that have well-defined procedural success paths (e.g., Human Failure Events 2 and 5) compared to those for which there was no clear unique procedural path (e.g., Human Failure Events 3 and 4). Generally, there was considerable variability in the assessment of execution tasks and credit for recovery, which suggests these are areas that deserve more attention in future versions of the method guidance and training. A consensus on procedural success paths and critical tasks did not always translate to consensus on the performance-influencing factors, scenario dynamics, or final human error probabilities. Conversely, although some teams produced the same or similar human error probabilities for a given human failure event, there was not always a consensus on the selected crew failure modes and performance-influencing factors.

However, there were also multiple examples of interanalyst consistency in the study. For example, some teams obtained the same or similar human error probabilities with an agreement on crew failure modes or performance-influencing factors. Moreover, there were cases where all the teams had a general consensus on the procedural success paths or critical tasks. This

points to evidence that IDHEAS AT-POWER provides an analysis framework that can enhance interanalyst consistency, but some methodological and guidance limitations can make it difficult to achieve interanalyst consistency throughout the IDHEAS AT-POWER analysis process.

The HRA process is subject to the influences of many interacting factors, which can cause variability in HRA results at each step of the process in complicated and subtle ways. One observation from the study was that variability among analysts in the early stages of the analysis propagated to subsequent steps, creating a sort of ripple effect, and compounding the variability in later stages of analysis. Since many factors can cause variability in HRA results, it is not realistic to eliminate all variability. In addition, variability does not necessarily indicate that errors were made in the analysis but can instead suggest uncertainty in the scenario dynamics. In some cases, variability is the natural result of analysts' uncertainty about how a scenario development influences operator responses and reflects differences in the inputs that analysts bring to their analyses, including assumptions, operations knowledge, and expectations of typical operator behavior. This highlights the importance of consistent information input to analysts and adequate justification of assumptions during the analysis. For example, the five analyst teams generally agreed on the procedural paths and associated cues for diagnosing the slow loss-of-coolant accident and making procedural transfers in Human Failure Event 5. The consistency can be attributed to the consistent timing and thermohydraulic information given to the analyst teams by the designated operator. When consistent input is unavailable or not well developed, it is reasonable to expect variability to arise as a function of the assumptions made by the analysts. Under such circumstances, the important issue is not whether variability can be avoided, but rather whether the method allows identification of the sources of the variability (i.e., good traceability).

Based on the discussion above, the study concludes that despite methodological and guidance limitations that can impede interanalyst consistency, a reasonable level of interanalyst consistency can be achieved with IDHEAS AT-POWER. The degree of consistency is expected to vary based on the complexity of the scenario, level of information available, and expertise of the analysts. In general, the variability observed in the study manifested in three aspects: analyst judgment in addressing scenario complexity and uncertainty, crew response diagram construction, and crew failure mode and performance-influencing factor evaluation. The latter two aspects are, to some extent, related to the first aspect in that scenario uncertainty can lead to variability in crew response diagram construction and crew failure mode and performance-influencing factor evaluation. The following subsections summarize the variability observed with respect to the three aspects and provide insights on areas for method improvement.

4.2.1 Analyst Judgment in Addressing Scenario Complexity and Uncertainty

No HRA method can be purely prescriptive; some amount of analyst judgment is necessary for analysts to address scenario complexity and uncertainty. In particular, analysts may rely more heavily on their judgment for novel scenarios, such as those that are not typically defined in PRAs. When there is lack of familiarity with a scenario, analysts tend to rely on their prior knowledge of procedures, operations, and other similar scenarios. Differences in prior knowledge and expectations between analysts can affect the assumptions made about operator performance, and thereby translate into greater interanalyst variability in HRA results. The analysts' assumptions about how operators would respond were sometimes so strong that the analysts were not able to reach a consensus on some aspects of the human failure events even after the discussion at the post-analysis workshop.

Since it is not realistic to eliminate analyst judgement in HRA, the important issue in addressing interanalyst variability caused by analyst judgment is to provide a framework for analysts to identify sources of uncertainty, improve consistency in judgment, document the judgment, and perform necessary sensitivity analyses. The level of traceability of the analysts' thought process can facilitate further review and discussion to potentially resolve differences in the analysis or gather more information to address areas of uncertainty.

It should be noted that some sources of complexity and uncertainty observed in the study were beyond the scope of IDHEAS AT-POWER. The analyses of Human Failure Events 3 and 4 were complicated by analysts' uncertainty regarding which of multiple procedural paths operators would choose. In some cases, multiple procedural path choices could potentially lead to success, but would result in different crew failure modes and performance-influencing factors affecting the likelihood of success. The analysts dealt with such a situation by making assumptions to simplify their analyses. The IDHEAS AT-POWER guidance suggests one possible approach to dealing with these types of complex scenarios by choosing a representative procedural path for the crew response diagram and identifying the assumptions made about the procedural path as a source of model uncertainty. An alternative resolution may be to analyze all the possible procedural paths on a case-by-case basis. See Section 4.6.3 and Appendix D for more discussion on the case-by-case approach to addressing procedural uncertainty.

4.2.2 Crew Response Diagram Construction

A crew response diagram node on the success path normally represents a high-level task 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. Hence, the crew response diagram will vary with the procedural path chosen to model crew success and be impacted by the uncertainty in the procedural path and associated critical tasks. This was most clear when there were multiple potential procedural paths, when analysts had different expectations of typical operators, and when they had different interpretations of the information from interviews with the designated operator.

When the teams chose the same procedural path, they sometimes decomposed the tasks differently (e.g., different task groupings) or identified different critical tasks. Some teams decomposed execution tasks into a lower level, which was not consistent with the method guidance as it was intended to be applied. Nevertheless, the difference in task decomposition alone did not seem to have a significant impact on the final human error probabilities in the study. However, it was noted that differences in task decomposition have the potential to change the human error probability by a factor of two or three, depending on the associated performance-influencing factors. Since each critical task is analyzed for its cognitive activities to determine applicable crew failure modes, different task groupings should result in the same set of applicable crew failure modes and the same final human error probability. The problem is associated primarily with defining what cognitive activities constitute status assessment, response planning, and execution, and the potential to miss or double count activities in different phases of operator response.

Another source for variability in the crew response diagram was modeling the viability of recovery, which has a potential impact on the quantitative results. As noted in Section 3.3, the teams in some cases did not provide sufficient documentation for why recovery was or was not considered. One reason for the variability might be that the approach to recovery in IDHEAS AT-POWER is different than some of the more commonly used HRA methods, and that the

guidance is not very clear on how to follow a failure path from a critical task through the procedures to identify possible recovery paths. Analysts may have also found it difficult to search for and identify recovery opportunities at this stage in the analysis because it required significant effort to search through possible alternative procedural paths and develop an understanding of how operators might respond differently if they initially failed to complete a critical task.

4.2.3 Crew Failure Mode and Performance-Influencing Factor Assessment

The identification of applicable crew failure modes and the assessment of the performance-influencing factors is based on the assessment of the cognitive activities constituting a critical task and the context under which the cognitive activities are performed.

The guidance for selecting applicable crew failure modes and determining performance influencing factor ratings rely, to some extent, on subjective descriptions rather than being based on concrete, objective, and measurable criteria. Feedback from the analysts indicated that they had difficulty in interpreting whether some crew failure modes were applicable, interpreting the guidance for selecting performance-influencing factor levels, and answering the associated reference questions.

When the guidance was not considered sufficient, analysts had to rely on their judgment in interpretation of crew failure mode scope and applicability for a particular situation. The subjectivity in analysts' interpretation of the guidance may become a potential source of interanalyst variability, which can be exacerbated by inadequate training. There were many cases in the study where the crew failure modes were interpreted in a way that was not consistent with the intent of the method. This led to situations where a particular effect was double counted, or crew failure modes were inappropriately selected. Similarly, for performance-influencing factors, there was considerable disagreement in judgment on whether the specific aspect of workload applicable to a crew failure mode was high or low, whether a procedure was complex or simple, and whether an execution task was straightforward or not. Some of the disagreement had a significant impact on the final human error probability.

Inconsistencies in the modeling of recovery and selection of recovery performance-influencing factors also contributed to variability in the results. It should be noted that when a recovery opportunity is identified for a critical task in the crew response diagram, it will be credited via the performance-influencing factor "Recovery Potential" if the selected crew failure mode(s) includes this performance-influencing factor. The teams were not always in agreement regarding identification of recovery opportunities in the crew response diagram. In addition, the teams were not always consistent in ensuring that when a recovery was modeled in the crew response diagram the associated "Recovery Potential" performance-influencing factor was credited, and vice versa.

4.3 Traceability

The study indicated that traceability is a strength of IDHEAS AT-POWER, which can be attributed to the method analysis framework and process. Constructing the crew response diagram and identifying critical tasks provides a process for analysts to decompose a human failure event and parse operating procedures in a traceable and systematic manner. The crew response diagram itself provides a graphical description of the procedural success path, what tasks are important, and when a failure can be potentially recovered.

The critical tasks identified by the analysts serve as the quantification unit of the IDHEAS AT-POWER method. The failure probability of a given critical task is determined by applicable crew failure modes and the ratings of associated performance-influencing factors. The use of decision trees establishes a clear link between the performance-influencing factor ratings and failure probabilities. This makes the derivation of the human error probabilities fully traceable and repeatable given the same quantification inputs. The important crew failure modes and important performance-influencing factors can be determined by examining the contributions of the crew failure modes and performance-influencing factors to the final human error probability.

The assessment of crew failure modes and performance-influencing factors is driven by the insights obtained in the scenario analysis. A list of questions is provided for each performance-influencing factor in a decision tree to help analysts judge the status of the performance-influencing factor. Although the questions do not necessarily represent all the circumstances or aspects related to the performance-influencing factor and some questions may not be applicable to specific scenarios, analysts' answers to the questions help to establish the link between the scenario analysis and the quantification inputs.

The method elements and analysis framework made it easy to pinpoint the sources of differences between different analysts. However, it should be noted that the ability to trace analysts' decision process on crew failure modes and performance-influencing factor ratings is, to some extent, a function of the quality of analysts' documentation of their decision process. Good documentation was particularly necessary when assessments were based on information not adequately covered by the performance-influencing factor reference questions or other method guidance. In addition to improvement of the guidance for crew failure mode and performance-influencing factor assessment, emphasis on the importance of documentation can help further enhance traceability.

4.4 Usability

On average, the analyst teams indicated that IDHEAS AT-POWER was somewhat difficult to learn and use, and extensive resources were needed to use the method (see discussion in Section 0). Several factors impacted the method's usability. First, it was time consuming to develop the narrative, crew response diagram, and timeline and document the analysis. Analysts also reported that there was some unnecessary redundancy when documenting details. On average, it took most teams about 38 hours to analyze one human failure event, which was considered much higher than the time needed with other HRA methods currently used by the NRC and industry. Even when accounting for time saved from repeated use of the method, analysts still expected a typical analysis to take, on average, 16 to 24 hours (see Table 3-7~~Table 3-7~~). It was believed that a computerized version of the tool could substantially reduce the amount of time needed to perform an analysis and redundancy in the documentation.

Analysts reported a significant learning curve when it came to assessing crew failure modes and performance-influencing factors. Understanding the intent of each crew failure mode and performance-influencing factor is a skill that requires practice and training and can be challenging for beginners. However, analysts believed that it would take less time as users become more familiar with the crew failure modes. In some cases, evaluation of crew failure modes and performance-influencing factors was difficult either due to inadequate guidance or because subjective judgment was needed.

It was also clear from observations of operator interviews and analysts' feedback that using the method required significant operations input for determining procedural paths, recovery potential, and timing. As a result, effective use of the method can be, to some degree, dependent on analysts' expertise in human performance and plant operations, or dependent on access to relevant expertise for conducting interviews.

The need for additional resources when using IDHEAS AT-POWER, as compared to other HRA methods, is partly due to the systematic process analysts must follow to perform the analysis. Rather than examining a set of characteristics of a human failure event at an overall level, it requires analysts to carefully parse procedures and collect HRA relevant information through operator interviews or other means to map out a procedural success path and identify critical tasks. Some of the detailed analysis elements built into IDHEAS AT-POWER can be bypassed when using other HRA methods. In addition, some HRA methods may be perceived as easier or less resource-intensive to use, but at the same time do not meet all the requirements for a detailed HRA analysis in the ASME/ANS PRA Standard [13]. The extra effort taken to develop the qualitative elements contributes to some of the strengths of IDHEAS AT-POWER. For example, it was agreed among the analyst teams that the method facilitates a detailed understanding of the unfolding of a scenario, the evolving perspective of operators, and how each critical task is performed and may fail as a function of the scenario evolution. When properly used, the method can enable many scenario-specific timing and performance issues to be identified and lead to a defendable basis for assessment of crew failure modes and performance-influencing factors. Careful documentation of the analysis process can be time consuming, but it also increases method traceability and facilitates a third-party review.

Although the results of the study suggest that IDHEAS AT-POWER is not particularly easy to learn and use compared to other HRA methods, the analysts viewed the method as very thorough, and appreciated that it encouraged the development of a deep understanding of scenario dynamics. As such, IDHEAS AT-POWER may be most appropriate for use by highly experienced HRA analysts when analyzing complex scenarios. The additional resource costs required to use the method may be offset by the benefits derived from the method's thoroughness and traceability.

4.5 Utility

It can be inferred from the testing that it is possible to derive insights from IDHEAS AT-POWER analysis results that may have relevance for training, plant design, procedure improvement, and risk management decisionmaking. This is because, as noted by the analyst teams, the analysis process aids the development of a thorough understanding of a scenario. For example, the careful parsing of the operating procedures for analyses of Human Failure Events 3 and 4 revealed the ambiguity in the procedures that could lead the operating crews to choose different procedural paths, depending on their training and interpretation of the procedure. This type of observation is a useful finding that could help improve the quality of operating procedures.

Similar to other performance-influencing factor/PSF-based HRA methods, the relative contributions of crew failure modes and performance-influencing factors to the final human error probabilities point to areas where error reduction is needed and where resources can be focused for improvement. For instance, all the analyst teams agreed that Crew Failure Mode SA1 (Data Misleading or Not Available) was the dominating failure mode and human error probability contributor in Human Failure Event 2. The decision tree associated with this crew failure mode illustrates the importance of having confirmatory indications of plant status to compensate for missing or inaccurate information. The utility of IDHEAS AT-POWER results is

clearly a function of the quality of the qualitative analysis. A carefully performed qualitative analysis is important to ensure a defendable basis for error reduction recommendations so that the recommendations are credible.

4.6 Additional Observations

In addition to the evaluation criteria described above, the project team had the following additional observations as a result of testing the IDHEAS AT-POWER guidance.

4.6.1 Sensitivity of Binary Decision Trees

IDHEAS AT-POWER, like some other HRA methods, uses decision trees to facilitate selection of performance-influencing factor levels. The decision tree approach to quantification can increase method traceability, but decision trees, particularly binary trees, have been criticized for their simplified representation of the real world. With a binary decision tree, as is used in IDHEAS AT-POWER, each performance-influencing factor has only two levels (e.g., high vs. low, good vs. bad, nominal vs. poor, or nominal vs. superior). From a qualitative point of view, this approach does not adequately reflect the fact that contextual conditions change on a continuous spectrum. From a quantitative point of view, a change in performance-influencing factor levels can lead to a significant change in the human error probability. For instance, although the five analyst teams agreed on the same dominating crew failure mode for Human Failure Event 2, their choices of three different paths on the same decision tree caused the human error probabilities of Teams 2 and 5 to be about one order of magnitude lower than those of Teams 1, 3, and 4. As a result, the binary decision trees can lead to large fluctuations in the results based on different interpretations of performance-influencing factor levels.

4.6.2 Cumulative Effects of Small Failure Probabilities

One of the fundamental steps of IDHEAS AT-POWER requires analysts to choose applicable crew failure modes from a predefined list. Each crew failure mode has an associated decision tree with the most relevant performance-influencing factors for that crew failure mode, and analysts must choose the performance-influencing factor level based on the scenario context. The human error probability for a human failure event is then calculated as the sum of the failure probabilities for all the applicable crew failure modes. When there are negative performance-influencing factors for some of the crew failure modes (i.e., factors that may increase the likelihood of human failure, like high workload, poor human system interface, or less-than-adequate training), the human error probability is likely to be controlled by those crew failure modes. Conversely, when most or all performance-influencing factors are in a nominal condition, the applicable crew failure modes can yield small failure probabilities such that none of the crew failure modes dominate the human error probability. However, the additive effect of the small failure probabilities can increase the human error probability as the number of applicable crew failure modes increases. The cumulative effect of these small failure probabilities may result in an overly conservative final human error probability for a scenario where most or all of the performance-influencing factors are nominal.

Most crew failure modes in IDHEAS AT-POWER yield a failure probability on the order of 10E-5 or lower when the lowest path on the crew failure mode decision tree is selected (i.e., when all or most of the performance-influencing factors are nominal), with the exception of Crew Failure

Modes AP2[4] (Misread or Skip Step in Procedure), SA1 (Data Misleading or Not Available), RP1 (Misinterpret Procedure), RP2 (Choose Inappropriate Strategy), and E3 (Failure to Initiate Execution), which produce a failure probability on the order of 10E-4 or even 10E-3. This implies that those failure modes are more likely to occur than others even when the performance-influencing factors are nominal. In particular, the failure probability associated with the lowest path of Crew Failure Mode E3 (Failure to Initiate Execution), which is intended for screening, is one to two orders of magnitude higher than the failure probabilities associated with the lowest path of other execution crew failure modes. This can easily cause the lowest path of Crew Failure Mode E3 (Failure to Initiate Execution) to dominate the execution human error probability or even the total human error probability, as observed multiple times in the study. In addition, during the study, analysts frequently selected Crew Failure Mode AP2 (Misread or Skip Step in Procedure) for most critical tasks. This is understandable in that the scope of IDHEAS AT-POWER always involves the use of operating procedures. Hence, it is possible that Crew Failure Mode AP2 can artificially inflate a human error probability when selected in an analysis of a human failure event where all performance-influencing factors are nominal.

4.6.3 Adaption to Address Scenario Aspects beyond Method Guidance

The study identified two instances where the analyst teams had to adapt IDHEAS AT-POWER to address some scenario aspects that were beyond the scope of the existing method guidance.

First, as discussed in Section 4.2.1, some sources of complexity and uncertainty in Human Failure Events 3 and 4 were beyond the scope of IDHEAS AT-POWER. When analyzing the two human failure events, some analyst teams encountered difficulty with performing the task analysis and constructing the crew response diagram because there was not a single well-defined procedural path that would lead the crew to success. In many cases, the crew's choice of procedural paths is not between the right path and the wrong one, because each path can lead to success. However, one option may not be optimal because it decreases the likelihood of success (i.e., increases the conditional human error probability). This type of decisionmaking between alternate success paths is not captured by the crew failure modes and not addressed in the method guidance. To address this gap, the analyst teams assumed and analyzed only one of the possible procedural paths. An alternative resolution may be to analyze all the possible procedural paths on a case-by-case basis to address the uncertainty in procedural paths. The human error probability for a particular path could then be assessed as a conditional failure probability given the relative probability of each case. Expert judgement would be needed to assess relative probability and derive a final human error probability using this approach. The project team (Team 5) attempted this strategy in revised versions of their analyses for Human Failure Events 3 and 4 (see Appendix D) but did not complete the analyses because the expert elicitation was deemed to be beyond the scope of the testing. The proposed alternative approach would be a more comprehensive analysis of a human failure event with multiple success paths but would likewise increase the level of effort to perform the analysis.

Second, there was an additional concern for Human Failure Events 3 and 4 in that some activities did not correspond clearly to one or more of the crew failure modes. One of the critical tasks identified by some analyst teams was to assess the time since seal cooling was lost; in

[4] The lowest path of the decision tree for Crew Failure Mode AP2 (crew failure scenario 14) yields a failure probability of 1.2E-04, which is higher than the failure probability for crew failure scenario 12 where not all the performance-influencing factors are nominal.

the procedure, there is a warning not to restore cooling if the cooling has been lost for 15 minutes without first isolating the seals. This task involves (1) an initial assessment of the elapsed time, and (2) an assessment of the elapsed time after the initial assessment is done if the initial assessment is less than 15 minutes. The initial assessment is in a sense a forensic activity that requires looking backwards to determine when the cooling became insufficient. There is no clear indication of when all cooling was lost, since it only became apparent after the fact when the bearing temperature alarms came in. While there is a situation assessment aspect to this activity, there is no crew failure mode that addresses the nature of this activity. Only Teams 1 and 5 explicitly considered the initial assessment activity in their analyses of the human failure events. They attempted to adapt the method to this activity by identifying Crew Failure Mode SA3 (Critical Data Misperceived) as an applicable crew failure mode. However, this crew failure mode was not intended for this type of forensic activity but was intended more for a situation where the information did not fit expectations. In addition, note that it is not clear if Crew Failure Mode SA3 is relevant for Human Failure Event 4. If the time elapsed since loss of all cooling is less than 15 minutes when the crew reaches Step 2 in Appendix C of AOP-018, a misperception would in fact increase the likelihood of success in tripping the reactor coolant pumps because the crew would go to Step 3 rather than Step 10.

Only Team 5 explicitly considered the second assessment activity in Human Failure Event 4. They modeled it as a time monitoring activity per a continuous procedural step while operators try to restore seal cooling. This activity seems to be sufficient for the time assessment task because, as discussed in the paragraph above, a failure in the initial assessment when the elapsed time is less than 15 minutes would in fact increase the likelihood of success in tripping the reactor coolant pumps. Treating the second assessment as a monitoring activity may be appropriate given that the operators should be aware of loss of all seal cooling after they enter AOP-018. That is, given that their initial assessment was that the time elapsed was less than 15 minutes, what they would be doing following that determination would be to monitor time per procedural guidance while trying to restore seal cooling. There does not seem to be clear guidance on how to treat this type of time monitoring activity and which crew failure mode(s) would be applicable to it. The team considered this as a nonexecution activity but used execution Crew Failure Mode E2 (Critical Data Not Checked with Appropriate Frequency) to capture the potential failure in this activity that would directly lead to not tripping the reactor coolant pumps. This is another example of adaption of the method to address scenario aspects beyond method guidance. Note that it could be argued that although the monitoring activity is, to some extent, a situation assessment, it is different from typical situation assessment activities and could be considered part of an execution task, because an important status assessment has been made at this point—the operators know they have no cooling.

4.6.4 Treatment of Execution

IDHEAS AT-POWER treats execution in a holistic manner. That is, multistep actions that comprise an overall execution task (e.g., feed and bleed, or cooldown and depressurize) are typically modeled as a single critical task on the crew response diagram. One merit of this approach is that it reduces the likelihood of obtaining unreasonably high human error probabilities, as can occur when assessing each individual execution step and then summing up each step's failure probability. However, there are also some disadvantages to this approach. First, IDHEAS AT-POWER divides execution tasks into two generic categories: simple and complex. There were multiple instances in the study where analysts disagreed on whether an execution task should be categorized as simple or complex based on their interpretation of the guidance. Analysts also expressed frustration over not being able to differentiate between execution tasks that both met the definition for complex, but that clearly had very different levels

of complexity. Currently, IDHEAS AT-POWER treats control actions (i.e., actions that require making adjustments and continuous monitoring as manipulations are carried out) as a special case of the complex task, except that recovery potential is not considered for control action failures because any corrections would be made as part of the evolution of the continuous monitoring and manipulation. Given the unique characteristics of control actions, the method may require a separate control action decision tree with its own set of performance-influencing factors and associated reference questions to address control action failures.

Second, although IDHEAS AT-POWER has a focus on the cognitive aspects of operator behavior, the holistic treatment of execution means that response implementation is treated as purely execution or implementation and analysts are not encouraged to explicitly address cognitive or operational demands during the execution of a response. Operators perform cognitive activities together with the collection of plant information through a scenario's evolution. These cognitive activities and information gathering enable operators to achieve two goals: (1) understand the plant situation and decide on the appropriate response, which may also be referred to as initial diagnosis, and (2) make decisions during the execution of the selected response plan. In current nuclear power plant operations, these cognitive activities are supported by emergency operating procedures (EOPs) and other procedures and occur while the operators are following emergency operating procedures. In a steam generator tube rupture scenario, identification of the ruptured steam generator is an example of initial diagnosis, whereas reactor coolant system cooldown and depressurization involve cognitive activity during execution, such as selection of appropriate cooldown rate and decision to stop cooldown or depressurization when the desired state is reached. An incorrect cooldown rate or a premature decision to stop cooldown or depressurization could lead to a failure to implement the action. Such examples illustrate how cognitive activities with goal (2) may lead to the execution failure of a given response. Although IDHEAS AT-POWER has a focus on the cognitive aspects of operator behavior (see Section 5.1.4), the holistic treatment of execution means that analysts are not required to explicitly address the cognitive demands during the execution of a response. This might lead to a failure to identify important performance-influencing factors and result in underestimation of human error probabilities.

Therefore, although the holistic approach to execution may be worthwhile for quantification purposes, there may also be benefit to initially decomposing execution to a more detailed level for a broad consideration of the conditions that could lead operators to fail. Based on the functional, cognitive, and procedural requirements of the execution task to be analyzed, the HRA analyst may determine at a later stage that the execution task can be treated holistically (e.g., when related decisions for some steps in the procedures create a dependency between the steps, or when decomposing the task is not necessary due to low probability of failure).

4.6.5 Assessment of Impact of Timing on Operator Performance

The timing of operator actions is explicitly treated in IDHEAS AT-POWER in several ways. For example, a timeline is constructed to assess the time window for a successful operator response as one of the response feasibility criteria and as part of the scenario analysis. There are also multiple ways that the effects of short time windows are represented in the quantification process. First, although there is no crew failure mode dedicated to capturing the effect of short time windows, the effect is partly accounted for in the performance-influencing factor for workload, which appears in multiple crew failure modes. Second, short time windows are also partly accounted for in recovery modeling: when the time available is short, no credit can be taken for recovery. Third, IDHEAS AT-POWER adopts a time-reliability model to capture the error probability for human failure events with short time windows. The testing did

not explicitly focus on human failure events with short time windows, and analysts were not asked to use the time-reliability model as part of their analyses. However, feedback from the analyst teams suggested that, in some cases, they did not feel that short time windows were adequately accounted for by the quantification process. That is, although some analysts thought that the short time window of a scenario should be an important performance driver, they did not feel that the impact of timing was fully represented in the quantification process. This may be because the time reliability model was not included as part of the testing. Nonetheless, the observation suggests a need for additional evaluation of the approaches to treating timing and consolidated guidance for coherent application of the approaches.

4.6.6 Applicability of Crew Failure Modes Based on Response Phases

Many of the analyst teams had some difficulty determining whether a crew failure mode was applicable to a critical task, particularly when the crew failure mode could apply to different response phases. All teams, including the project team, used the Crew Failure Mode AP-2 "Misread or Skip Step in Procedure" for execution tasks. However, the method guidance indicates that Crew Failure Mode AP-2 is not applicable for execution when the procedural steps are integral to the guidance for execution, because this failure mode has been implicitly considered in the failure probability associated with execution crew failure modes. However, care must be taken in defining the critical task and identifying the activities associated with the crew response diagram node for execution. In some cases, one of the activities associated with what is nominally called an execution task may involve a procedural step involving a decision such as, "If parameter X is less than Y then execute…" In such a case, it may be appropriate to include the Crew Failure Mode AP-2 as a potential crew failure mode.

This confusion may be due to how Crew Failure Mode AP-2 was presented in the training and labeled as an "All Phase" crew failure mode, and the fact that it is generally not applicable to execution tasks may not have been emphasized. In several cases, the use of Crew Failure Mode AP-2 increased the execution-related human error probability by one order of magnitude but did not significantly impact the final human error probability in most cases due to other dominating crew failure modes and performance-influencing factors.

On the other hand, although explicit instructions were given in the training that status assessment or response planning crew failure modes were not applicable to execution tasks, some teams selected some of those crew failure modes for some execution tasks. In some cases, the inappropriately selected crew failure modes were among the dominating contributors to the final human error probability.

4.6.7 Application of Recovery

The consistent application of recovery seemed to be a challenge for multiple teams when implementing the method guidance. Some teams credited recovery that was not identified on a crew response diagram, or they identified a recovery path on a crew response diagram but did not credit it in crew failure mode assessment. In one case the analyst team followed the method guidance, but inappropriately credited recovery because of how they identified critical tasks in their crew response diagram. In their analysis of Human Failure Event 3, Team 3 combined two critical tasks (i.e., identification of loss of seal cooling and opening FCV-626) under one crew response diagram node (see more details in Section 3.3.3). The combination was not inconsistent with method guidance because the team assessed crew failure modes for each critical task. The team also identified a recovery path for this node on the crew response diagram; however, the recovery path was misleading in that it suggested that the recovery path

would recover the potential failure of both critical tasks included in the crew response diagram node. The recovery path only recovered the identification of loss of seal cooling. Because the method guidance tells analysts to credit recovery potential on a decision tree if a recovery path is identified for a corresponding crew response diagram node, the team inappropriately credited recovery for both tasks.

4.7 Lessons Learned from Testing

In addition to the insights regarding IDHEAS AT-POWER, the study produced lessons learned about the testing methodology. Some of these lessons reflect limitations in the experimental design, which impacted the evaluation of the IDHEAS AT-POWER method. Given that this study is a test of a new HRA method prior to its publication as ready-for-general-use, lessons from the conduct of the testing can be beneficial for future studies of this nature.

4.7.1 Selection of Testing Scenarios and Definition of Human Failure Events

One objective when it came to selecting the testing scenarios was to include scenarios at varying levels of complexity. For instance, Human Failure Event 1 was selected because it was a straightforward scenario, and the other human failure events were clearly more complicated than Human Failure Event 1. The testing results confirmed this differentiation: among the five human failure events, the operator response to Human Failure Event 1 was unanimously agreed to be the least challenging. However, there was not a clear differentiation in difficulty among the other human failure events selected for testing. Even after debating the difficulty of the human failure events during the post-analysis workshop, the analyst teams and project team could not reach full consensus on the difficulty rankings for Human Failure Events 2-5. In some cases, the lack of consensus was because human failure events were considered to be at the same difficulty level, and in other cases it seemed that analyst teams did not have agreement on the scenario dynamics and performance-influencing factors. It would be desirable for future studies to consider the difficulty level of each human failure event relative to the other human failure events selected for testing to ensure that the HRA method is able to consistently discriminate among human failure events at varying levels of difficulty.

Although caution was taken to ensure that human failure events were clearly defined, there was still some ambiguity in human failure event definitions. Analyst teams asked about the boundaries of the actions required for successful response. For example, the lack of clarity of the boundaries in the Human Failure Event 5 definition impacted the teams' interpretation of the time window, which in turn affected the teams' judgment regarding the potential for recovery. Some teams interpreted the definition as failure to start depressurizing the reactor coolant system during a slow loss-of-coolant accident, whereas other teams interpreted it as failure to complete depressurizing the reactor coolant system.

Scenario 3 was selected partly due to the considerations of the benefits of complicated scenarios for testing an HRA method. However, some unanticipated factors caused the scenario to be too complicated to be an ideal testing scenario, which may have limited study findings on method ability to identify failure modes in complicated scenarios. The quality of some operating procedures for the scenario were not adequate relative to today's standards and analyst teams had difficulty interpreting them. This caused unnecessary distraction and increased the difficulty of the analysis.

Similar to what was mentioned above, the boundary conditions for Human Failure Events 4 and 5 were not clearly defined, in part because they were dependent on Human Failure Event 3. The analysts needed to assume some failures to get to the point at which the responses required for the failure events associated with Human Failure Event 4 and 5 were appropriate. As a result, the teams differed in the starting point of their analyses. In addition, Human Failure Events 3 and 4 were so intertwined it was difficult to analyze them as independent events, which is what the analyst teams were asked to do.

Furthermore, as discussed in Sections 4.2.1 and 4.6.3, the analysts identified multiple procedural paths that the operators could take to achieve a successful response for Human Failure Events 3 and 4. Because IDHEAS AT-POWER did not have guidance for assessing multiple procedural paths, the analyst teams chose to make an assumption regarding which path the operators would take. The lack of a single, well-defined procedural path complicated the analyses of Human Failure Events 3 and 4 and contributed to additional interanalyst variability in the results. Although this was identified to be a gap for future method development, it was beyond the current scope of IDHEAS AT-POWER, and inadvertently increased the variability in the testing results.

Another limitation of the study was the lack of empirically validated scenarios to test IDHEAS AT-POWER. Although Scenarios 1 and 2 were simulated on a nuclear power plant simulator, the utility of the simulator data was limited because the scenarios, especially Scenario 1, did not involve many challenges to test the method's ability to identify performance issues. Moreover, the uncertainty bounds obtained from the simulator data were very large and thus not very informative for assessing the validity of the human error probabilities estimated using IDHEAS AT-POWER. As a result, the study yielded limited insights on whether IDHEAS AT-POWER can produce valid human error probabilities. This limitation is also applicable to the validation of other HRA methods. The ideal would be to establish a bank of testing scenarios with validated human error probabilities using empirical data to use for validating HRA methods.

4.7.2 Impact of Analyst Team Differences on Testing Results

While evaluating the study, it became clear that some variables that were not fully controlled within the study had an impact on the testing results. Differences between the analyst teams made it difficult to determine whether observed differences in the results were due to method weaknesses or analysts' skill in implementing the method. Given constraints on the number of analysts that we were able to recruit for the study, variations in experience and areas of expertise, and time available to participate in the testing, it was not possible to design a between-subjects study with large numbers of equally skilled teams of analysts. The implication is that achieving valid and reliable HRA results requires not only a good HRA method, but also a skilled HRA user to properly apply the method.

Although an effort was made to ensure that each team collectively had adequate levels of experience in HRA, PRA, and nuclear power plant operations, there was still some significant variability. Teams with less PRA experience found it more challenging to develop an understanding of scenario dynamics, particularly for more complex scenarios. Teams with relatively less operations knowledge tended to rely more on the designated operator to identify procedural paths, timing, and recovery factors. Additionally, analysts with more HRA experience seemed better able to formulate questions in advance of the operator interviews to facilitate developing the crew response diagram and identifying applicable crew failure modes and associated performance-influencing factor levels.

Other between-team differences included analysts' knowledge of the method and skill in applying the method. Knowledge and skill were initially controlled for by requiring all analysts to participate in the same in-person training on the IDHEAS AT-POWER method. Given that this was a new HRA method, all the analysts lacked prior experience with the method. In one sense, lack of prior experience was a positive aspect of the study because all analysts began with the same baseline level of knowledge and received the same information about the method. However, given the complexity of the IDHEAS AT-POWER process, there was a significant learning curve for analysts to overcome to fully understand the method. Even highly experienced HRA analysts found it somewhat difficult to learn the method. In addition, due to last minute scheduling conflicts, some analysts were not able to attend all the training in person and instead had to rely on the study information package, training slides, and their team members to learn the method. Differences in analysts' prior HRA experience, including experience with HRA methods that are similar to IDHEAS AT-POWER, likely contributed to differences in learning and applying this new method.

Although two full days were allotted to classroom-style training on IDHEAS AT-POWER, some aspects of the method were either overlooked or not stressed enough during the training, which was then reflected in how the analysts used the method. For instance, although the holistic treatment of execution tasks was covered in the training, it was not emphasized enough to eliminate differences in how analysts decomposed the execution tasks in the testing scenarios. In addition, the presentation of Crew Failure Mode AP-2 as an "all phase" crew failure mode during training may have contributed to confusion regarding its lack of applicability for execution tasks.

In addition to the classroom training, analysts were provided with additional background material to facilitate learning and using IDHEAS AT-POWER, including a lengthy IDHEAS AT-POWER report. It was clear from discussions with the analyst teams during the post-analysis workshop that there were substantial differences between analysts in terms of the extent to which they referenced the IDHEAS AT-POWER report. Although all the teams generally followed the method guidance, some teams displayed greater attention to the details of the method guidance and demonstrated greater skill in method implementation. Some teams also seemed to rely more heavily on the shortened reference documents provided for convenience (e.g., the condensed list of crew failure mode decision trees). These reference documents were not intended to replace the guidance found in the method report, and over-reliance on the shortened reference documents may have led some teams to incorrectly interpret some aspects of the method, such as selection of crew failure modes, selection of performance-influencing factor levels, and appropriately crediting recovery.

4.8 Summary

Overall, the results of the testing indicate that IDHEAS AT-POWER provides a structured analysis framework and traceable quantification approach to HRA. There were some instances where the method was not applied consistently with method guidance, but the analyst teams generally followed the analysis process and applied the method as intended. Although interanalyst variability was not eliminated, the human error probabilities estimated with the method were not inconsistent with simulator data and converged with other HRA methods' estimations in the U.S. Empirical Study. The method exhibited the ability to capture a broad range of failure modes, contextual conditions, and influences on behavior associated with the difficult operator actions and complex scenarios in the study. As a result, the method has the capability to translate qualitative findings into reasonable human error probabilities.

The use of crew response diagrams, crew failure modes, and decision trees promoted good traceability, which, with good documentation, made it easy to pinpoint differences between analysts. The analysts agreed that the method required careful parsing of procedures and development of a detailed narrative, which can be easily bypassed when using other methods. This contributed to both strengths and weaknesses of the method. A carefully performed analysis can lead to a more defendable basis for assessing scenario-specific performance issues and influencing factors, which is especially important for complex scenarios. Moreover, the detailed analysis can identify areas for operator performance improvement, which increases the utility of the method. The documentation requirement also enhances traceability, which is important for a third-party reviewer to identify sources of interanalyst variability, assess whether the rationale underlying the analysis is reasonable, and evaluate the impact of the assumptions made to address uncertainty in the analysis. Conversely, the performance and documentation of the detailed analysis can be resource intensive in terms of time and operations input, impacting method usability. However, the benefits of the detailed analysis may outweigh the additional resource costs for complex, cognitively demanding scenarios where traceability and utility are critically important. In addition, it is believed that the resource requirements can be reduced with a computerized tool and elimination of redundant documentation.

The method was not particularly easy to learn or use, especially for beginners. Understanding the scope and applicability of each crew failure mode and performance-influencing factor proved to be challenging for the analysts. In addition, the detailed analysis of procedural steps to identify the critical tasks for a successful response and assessment of the scenario context to evaluate potential crew failure modes and performance-influencing factors required significant operations knowledge. This highlights the importance of adequate training and practice for analysts to efficiently apply the method, and operations input to appropriately apply the method.

There was some degree of interanalyst variability in the testing results, which was not consistent across the human failure events. The estimated human error probabilities varied by at least one order of magnitude across teams. Even when teams derived similar final human error probabilities, there were often variations in the chosen crew failure modes or performance-influencing factors. In some cases, the consensus on procedural success paths did not translate to complete agreement on the final human error probabilities. However, there was also significant evidence of interanalyst consistency across various steps of the analysis process. Further, it should be acknowledged that the HRA process is subject to the influences of many interacting factors, which can cause variability in HRA results at each step of the process in complicated and subtle ways and then propagate to subsequent steps. Second, although experimental controls were taken to minimize undesired influences, some effects were unanticipated, difficult to control, or even unavoidable within the constraints of the study. Moreover, it is unrealistic to expect to completely eliminate variability in a process that inherently requires subjective judgment. Therefore, although the results suggest that interanalyst variability can still arise with IDHEAS AT-POWER, there was also evidence that the traceability of the method allows for homing in on the exact points of disagreement between analysts, which provides a potential basis for resolution of conflicting viewpoints. Improvements in the method guidance, consistent training, and additional demonstrations of the method on a range of scenarios is likely to improve consistency over time.

5 RECOMMENDATIONS

This report documents a holistic test of IDHEAS AT-POWER. By allowing analysts to go through the entire HRA process, the test indicated where variability can occur in the analysis and identified potential gaps and areas for improvement. Based on the discussion in the previous chapters, recommendations are made below with respect to training, method guidance improvement, and future method development.

5.1 Training and Method Guidance Improvement

As revealed in the study, adequate training and sufficient method guidance is important for successful application of IDHEAS AT-POWER. Although analysts quickly understood the general method framework, it was challenging to fully understand the method details to apply the method properly and efficiently. Training and guidance may be improved by focusing on (1) aspects that are unique to IDHEAS AT-POWER or similar but different from other HRA methods, and (2) method nuances or circumstances where extra caution is needed in method implementation. Furthermore, time and practice are needed for analysts to fully understand the method guidance. Recommendations for improving training and guidance follow.

5.1.1 Crew Response Diagram Construction and Task Decomposition

The analysts have the latitude to use a crew response diagram node to represent either one critical task or a group of critical tasks. However, crew failure modes are assessed for each critical task regardless of how a critical task is represented by a crew response diagram node. Clarification is needed on the definitions of the concepts, how they are related, and why both concepts are needed. Including additional examples in training and in a user's manual for analysts will clarify these concepts.

The caution on recovery modeling for situations where multiple critical tasks are grouped under one crew response diagram node should be emphasized in guidance and training. When a recovery path is shown on a crew response diagram for a node that represents several critical tasks, it can be misleading if the recovery path only recovers the failures of some of the critical tasks represented by the crew response diagram node. Under such circumstances, it may be advisable to separate critical tasks into separate nodes to account for differences in recovery opportunities.

The identification of critical tasks is particularly important in IDHEAS AT-POWER because the critical tasks become the quantification unit for the method. A lack of clarity regarding what constitutes a critical task can lead to ambiguity regarding the most appropriate level of task decomposition. The testing suggested that the level of task decomposition was a significant contributor to interanalyst variability and has a potential to impact the human error probability. Although task decomposition is a common issue in HRA and, to some extent, considered as an art and dependent upon analyst skills, improved guidance would be helpful for consistent application of the method.

5.1.2 Execution Action Categorization and Holistic Treatment

Execution actions are divided into two generic categories: simple and complex. Additional clarification on the definition of each category is necessary to avoid ambiguity in the interpretation of the definition for consistent categorization of execution actions.

Section 4.6.3 discussed that it was not clear how to model a time monitoring activity in Human Failure Event 4. To some extent, this activity involves status assessment, but it is different from typical situation assessment activities because an important status assessment has already been made. Thus, it raises a question whether it is reasonable to model this activity or other similar activities as part of an execution task, which calls for clarification in method guidance.

It needs to be stressed in training that execution actions are to be treated in an integral holistic manner when using IDHEAS AT-POWER. As discussed in Section 4.6.4, there are concerns about this approach despite its merits. It is recommended that the concerns about the approach be explained clearly in method guidance so that analysts are fully aware of the potential limitations of the approach and apply it appropriately. Section 4.6.4 indicated that it may initially be useful to decompose execution to a reasonably detailed level for a broad consideration of the conditions that could lead operators to fail. Based on the functional, cognitive, and procedural requirements of the execution task to be analyzed, it may be decided later that the execution task should be treated holistically (e.g., when related decisions for some steps in the procedures create a dependency between the steps) or that it is not necessary to decompose the execution task into a detailed level for quantification purposes.

5.1.3 Crew Failure Mode and Performance-Influencing Factor Assessment

Additional clarification and concrete examples should be considered to minimize ambiguity in crew failure mode definitions and help analysts correctly interpret crew failure mode scope and applicability. For instance, providing examples to distinguish between Crew Failure Mode E1 (Delay Implementation), which is a strategic decision to delay execution, and Crew Failure Mode E3 (Failure to Initiate Response), which is a lapse (i.e., forgetting to begin the response). Not having a clear understanding of the applicability of a crew failure mode can lead to an inappropriate use of the crew failure mode. This may be more likely when the cognitive activity identified as being critical for success is not captured in any of the IDHEAS crew failure modes. An example of this might be the prioritization of responses, where a response may not be attended to because it is considered to be of lower priority. This was considered by some teams for Human Failure Event 3 in the case of the loss of CCW alarm, and one team chose the Crew Failure Mode SA1 (Data Misleading or Not Available) to represent this nonresponse. However, this nonresponse is not a failure per se, but a choice as discussed in Section 4.6.3 and Appendix D. The Crew Failure Mode SA1 (Data Mislead or Not Available) was created to address the situation where a piece of data taken at face value would lead to a response that was incorrect, and the decision tree addresses the likelihood of confirmation of the plant status before responding but was not intended to apply to a choice of strategy.

The need for additional clarification and examples also applies to performance-influencing factors, like those that appear in multiple crew failure modes, such as workload, and represent different aspects of the performance-influencing factor. Given that workload is such a broad concept, the definition accompanying the workload performance-influencing factor in various crew failure mode decision trees should alert analysts to the specific aspects of workload that are expected to have an influence on the crew failure mode.

Providing more objective criteria for assessing performance-influencing factor levels may reduce the interanalyst variability arising from differences in analyst's interpretations of the guidance. Due to the binary nature of the decision trees, clear definition of each binary state of each performance-influencing factor is important to calibrate the anchor or reference point that analysts should use to determine a performance-influencing factor's rating. Some performance-influencing factors, such as workload, represent different aspects of the performance-influencing factor when appearing in multiple crew failure modes.

For improved usability, some reference questions for performance-influencing factor assessment should be rephrased with simple language (e.g., avoiding double negatives). In addition, the terminology used to denote different performance-influencing factor levels should be consistent to aid analysts in distinguishing nominal or expected conditions when a performance-influencing factor is included as a compensatory factor versus a negative contributor to the failure mode. For example, work practices is included as a compensatory factor for Crew Failure Mode E-5 (Failure to Correctly Execute Response (Complex Task)), but the nominal performance-influencing factor level (i.e., the expected level if compensatory work practices are not present) was labelled as "poor," whereas the presence of compensatory work practices was labelled as "good." Conversely, training is included as a negative performance-influencing factor for Crew Failure Mode E-5 and nominal training was labelled as "good," whereas inadequate training is labelled as "poor."[5]

Since the performance-influencing factor assessment guidance represents the current state of knowledge regarding the factors that need to be considered to determine performance-influencing factor levels, the guidance should also be updated when necessary.

5.1.4 Recovery Modeling

In general, there are three categories of recovery for a given human failure event: immediate recovery, recovery prompted by new cues, and long-term recovery. How each category is defined and treated in IDHEAS AT-POWER should be explained clearly in guidance and emphasized in training. It is also worthwhile to provide caution on rules of crediting recovery opportunities. For example, a critical task may fail due to multiple crew failure modes; therefore, the recovery opportunities of the failure of the critical task should be assessed for each crew failure mode before credit is given via the Recovery Potential performance-influencing factor. Another special case is when using Crew Failure Mode E-5 (Failure to Correctly Execute Response (Complex Task)) to model complex control actions analysts should not credit the recovery potential performance-influencing factor. The guidance states that the recovery potential performance-influencing factor 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. Furthermore, as discussed earlier in this chapter, caution should be taken when giving credit for recovery of the failure of multiple critical tasks that are grouped under one crew response diagram node.

In some cases, the identification of recovery opportunities, particularly from errors of commission, can be difficult. It would be helpful to provide additional guidance on how to follow a failure path from a critical task through the procedures to identify possible recovery paths.

---

[5] Note that based on early feedback from the testing, some of the performance-influencing factor labels in the decision trees were revised in the final IDHEAS AT-POWER report.

5.1.5 Guidance Materials

The IDHEAS AT-POWER report is the primary source for understanding how the method developers intended for IDHEAS AT-POWER to be used. While planning the testing, it became clear that the report was not necessarily designed as a step-by-step user manual. Additional materials were developed for the testing to tailor the information in the report into training materials, quick reference guides, and templates for documenting results. Although the analysts found these materials helpful, it was noted that teams sometimes misinterpreted the guidance based on the shortened reference materials and did not consistently refer to the source report. The IDHEAS AT-POWER report would benefit from the development of a companion user manual designed specifically for use by HRA analysts seeking to implement the method. At the same time, care should be taken to ensure that the user manual is easy to use, yet comprehensive enough to facilitate use of the method as intended. The user manual and other guidance materials should include specific references back to the source report for more detailed information about various parts of the IDHEAS AT-POWER method.

5.2 Future Method Development

Several methodological limitations and issues were observed in the study. Resolutions to the limitations and issues require future method development and evaluation effort beyond improvement in training and existing method guidance. Below are some recommendations.

5.2.1 Supplementary Crew Failure Modes

Additional crew failure modes should be considered to supplement the current list of crew failure modes in IDHEAS AT-POWER. In particular, refinement of the decision tree for the execution crew failure mode to address control actions should be explored. Currently, control actions that would require making adjustments and involve continuous monitoring are treated as a special case of the complex execution crew failure mode. Additionally, as pointed out in Section 4.6.3, there are no crew failure modes that address (1) forensic activities that requires looking backwards to determine the status of a parameter, or (2) monitoring activities that do not involve important situation assessment. Development of supplementary crew failure modes to address such limitations may increase the completeness of the crew failure mode list and improve the capability of the method to address complex scenarios.

5.2.2 Evaluation of Failure Probabilities of Crew Failure Mode Failure Scenarios

The failure probabilities for each failure scenario on the decision trees were derived from expert elicitation. The self-consistency and reasonableness of the probabilities can impact the validity of the method. The concerns with the failure probabilities of the lowest paths of the decision trees for Crew Failure Mode E3 (Fail to Initiate Execution) and Crew Failure Mode AP2 (Misread or Skip Critical Steps in Procedure) suggest that it may be necessary to (1) systematically evaluate the failure probabilities, and (2) refine some decision trees to avoid the situation where the lowest probabilities of the decision trees can easily dominate the final human error probability when most or all performance-influencing factors are nominal (see discussion in Section 4.6.2). Future calibration of the probabilities might be accomplished through benchmarking the probabilities against established human performance data.

5.2.3 Evaluation of Additive Effects of Small Human Error Probabilities

As discussed in Section 4.6.2, the method developers should evaluate whether the additive effects of small failure probabilities artificially inflates the final human error probability for a human failure event. The additive effects of small human error probabilities may be particularly problematic when most or all performance-influencing factors are in a nominal condition.

5.2.4 Computerization of IDHEAS AT-POWER

Usability can be improved by eliminating unnecessary redundancy in the documentation. A computer-based tool is expected to be able to substantially reduce the amount of time needed to perform an analysis with IDHEAS AT-POWER by simplifying the process of developing the crew response diagram and timeline and by facilitating analysis documentation.

5.2.5 Evaluation of Holistic Treatment of Execution

Given the concerns over the holistic approach to treating execution (see the discussion in Section 4.6.4), further evaluation of this approach is necessary to fully understand its advantages and potential weaknesses to best inform method users.

5.2.6 Evaluation of the Case-by-Case Analysis Approach to Addressing Uncertainty in Procedural Paths

A case-by-case analysis approach has been proposed to address scenarios where there is uncertainty due to multiple potential procedural success paths (see Section 4.6.3 and Appendix D). However, it is acknowledged that this approach would increase the complexity of a human reliability analysis using IDHEAS AT-POWER, and likewise increase the level of effort needed to perform a comprehensive analysis. Further evaluation of the proposed approach is recommended to enhance the method's capability to address complex scenarios.

5.2.7 Future Method Assessment of IDHEAS AT-POWER

As indicated in the study, some variables were difficult to fully control and may have influenced the results. For instance, differences between the analyst teams likely increased the observed interanalyst variability. Challenges with some the scenarios also made the testing more difficult than anticipated (e.g., the difficulties interpreting the procedures used in Scenario 3 and multiple procedural success paths for Human Failure Events 3 and 4). Furthermore, several method elements were not included in the study scope (e.g., time reliability analysis, dependency analysis, etc.). Additional assessment of the method in the future is necessary for more conclusive findings about method performance. One benefit of the present study is that it identified several lessons learned. Future studies should consider these lessons to better control for undesirable effects and gain more flexibility in manipulating experimental conditions. Of course, if resources permit, another test with a revised method, more scenarios with a broader range of levels of complexity, and a greater number of analyst teams would be worthwhile to pursue.

6 REFERENCES

[1] Xing, J., Parry, G., Presley, M., Forester, J., Hendrickson, S., & Dang, V. (2016). An Integrated Human Event Analysis System (IDHEAS) for Nuclear Power Plant Internal Events At-Power Application. NUREG-2199, Vol.1., U.S. Nuclear Regulatory Commission: Washington, DC (ADAMS ML17073A041).

[2] Forester, J., Liao, H., Dang, V., Bye, A., Lois, E., Presley, M., Marble, J., Nowell, R., Broberg, H., Hildebrandt, M., Hallbert, B., & Morgan, T. (2016). The US HRA Empirical Study – Assessment of HRA Method Predictions against Operating Crew Performance on a US Nuclear Power Plant Simulator. NUREG-2156. U.S. Nuclear Regulatory Commission: Washington, DC (ADAMS ML16179A124).

[3] Forester, J., Dang, V., Bye, A., Lois, E., Massaiu, S., Broberg, H., Braarud, P., Boring, R., Mannisto, I., Liao, H., Julius, J., Parry, G., Nelson, P. (2014). The International HRA Empirical Study – Lessons Learned from Comparing HRA Methods Predictions to HAMMLAB Simulator Data. NUREG-2127. U.S. Nuclear Regulatory Commission: Washington, DC (ADAMS ML14227A197).

[4] Poucet A. (1989). Human factors reliability benchmark exercise, Final Report, EUR 12222. Ispra: CEC-JRC.

[5] Boring, R., Hendrickson, S., Forester, J., Tran T., & Lois, E. (2010). Issues in Benchmarking Human Reliability Analysis Methods: A Literature Review. Reliability Engineering and System Safety, 95, 591-605.

[6] Kirwan, B. (1996). The Validation of Three Human Reliability Quantification Techniques – THERP, HEART and JHEDI: Part I – Techniques Descriptions and Validation Issues. Applied Ergonomics, 27(6), 359-373.

[7] Kirwan, B. (1996). The Validation of Three Human Reliability Quantification Techniques – THERP, HEART and JHEDI: Part II – Results of Validation. Applied Ergonomics, 28(1), 17-25.

[8] Kirwan, B. (1996). The Validation of Three Human Reliability Quantification Techniques – THERP, HEART and JHEDI: Part III – Practical Aspects of the Usage of the Techniques. Applied Ergonomics, 28(1), 27-39.

[9] Kirwan, B. (1997). Validation of Human Reliability Assessment Techniques: Part 1 – Validation Issues. Safety Science, 27(1), 25-41.

[10] Kirwan, B. (1997). Validation of Human Reliability Assessment Techniques: Part 2 – Validation Results. Safety Science, 27(1), 43-75.

[11] HRA Calculator v. 5.1. EPRI, Palo Alto, CA: 2014. 3002003149.

[12] Gertman, D., Blackman, H., Marble, J., Byers, J., Haney, L., & Smith, C. (2005): “The SPAR-H Human Reliability Analysis Method,” NUREG/CR-6883. U.S. Nuclear Regulatory Commission: Washington, DC.

[13] American Society of Mechanical Engineers/American Nuclear Society (ASME/ANS), ASME/ANS RA Sa 2009, “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” Addendum A to RA S 2008, ASME, New York, NY, February 2009.

APPENDIX A
INFORMATION PACKAGE DESCRIPTION

Below is a list of the materials included in the information package that was provided to the analyst teams at the beginning of the study. The information package is too large to include in its entirety, so only portions of the package are included in the sub-sections of this appendix.

Table A-1 Table of Contents for Testing Information Package

Tab	Label	Description
1	Workshop Agenda	Agenda for the training workshop.
2	Overview and Instructions	Background to the testing project and instructions to the HRA analyst teams.
3	Testing Scenario Descriptions	Descriptions of the scenarios and associated HFEs that the HRA testing teams will analyze using IDHEAS AT-POWER.
4	Post-Analysis Questionnaire	Questionnaire to be completed by HRA analyst teams. Complete Section 1 after analyzing each individual HFE. Complete Section 2 after all HFEs have been analyzed.
5	Tutorial Part 1 – Introduction	Training slides presenting an introduction and overview to IDHEAS AT-POWER.
6	Tutorial Part 2 – CFMs and decision trees	Training slides presenting each of the Crew Failure Modes (CFMs) and associated decision trees.
7	Tutorial Part 3 – Examples	Training slides presenting example applications of the IDHEAS method.
8	IDHEAS AT-POWER Reference Material	Detailed report on the development of IDHEAS AT-POWER and its various components. Please refer to this report when additional guidance is needed beyond what was covered in the tutorials.
9	Attachment 1 – CFMs and decision trees	Guidance on selecting Crew Failure Modes (CFMs) and choosing paths in the CFM decision trees.
10	Attachment 2 – Glossary of Terms	Glossary of common terms used in HRA and IDHEAS AT-POWER.
11	Attachment 3 – Workload Assessment	Guidance for conducting a workload assessment. It may be helpful when assessing workload as a performance influencing factor (PIF) in selected CFMs.
12	Documentation Template	Template for use in documenting IDHEAS AT-POWER results. **Word file included on CD for ease of use.**
13	Example IDHEAS AT-POWER Report	Example report using the template to demonstrate how to document the IDHEAS AT-POWER analysis.
14	Procedures for Training	Selected procedures from a 4 loop Westinghouse plant. These will be used in the example presented in the IDHEAS AT-POWER Tutorial – Part 3.
15	Scenario 1 & 2 Procedures and Plant Information	**AVAILABLE ON CD ONLY.** Additional plant information and procedures to assist with analyzing Scenario 1 and 2.
16	Scenario 3 Procedures and Plant Information	**AVAILABLE ON CD ONLY.** Additional plant information and procedures to assist with analyzing Scenario 3.

A.1 Study Overview and Instructions

This section includes the overview and instructions that were provided to the analysts at the beginning of the study.

A.1.1 Background

The Integrated Human Event Analysis System (IDHEAS) is a new human reliability analysis (HRA) method developed by the Nuclear Regulatory Commission (NRC) in collaboration with the Electric Power Research Institute (EPRI). Many HRA methods currently exist to evaluate human performance as part of a Probabilistic Risk Assessment (PRA). However, there is evidence that HRA results can vary substantially, depending on the selected method and the way different analysts apply a particular method. The motivation for developing IDHEAS was to integrate the recognized strengths of existing HRA methods, provide enhanced guidance to address identified weaknesses, and incorporate state-of-the-art knowledge of why and how humans make errors in complex cognitive tasks. The IDHEAS method was developed specifically for analyzing procedure-based operator actions in a nuclear power plant (NPP) context when responding to internal, at-power events.

The purpose of this study is to pilot test the IDHEAS method and evaluate its use for HRA applications. Experience from the development of other complex methods, such as those used for plant fire modeling and analysis, have demonstrated the need for comprehensive piloting of new methods before deployment. The Advisory Committee for Reactor Safeguards (ACRS) recommended that the NRC staff conduct formal testing of IDHEAS with multiple teams of analysts who have a range of practical experience with evaluating human performance in PRA applications. Each team should evaluate the same set of PRA event scenarios that cover a range of human actions and anticipated crew failure modes, and the testing should demonstrate the advantages and limitations of the method with respect to state-of-practice HRA methods used by the NRC.

A.1.2 Instructions to HRA Analyst Teams

A.1.2.1 Review the Information Package

Each HRA analyst should become familiar with the contents of this information package. It includes the testing materials, training materials, and background information on the IDHEAS method. HRA analyst teams will be given time on Day 3 of the IDHEAS Testing Workshop to review the testing materials together, plan a strategy for completing the analyses, and ask clarifying questions.

A.1.2.2 Prepare Questions for Data Gathering

Each team will need to use the IDHEAS guidance to gather data about the HFEs they will analyze. The information package includes background information, plant procedures, and diagrams to assist with the analysis. Teams will also have an opportunity to interview a designated operations subject matter expert (SME), who can answer questions that an HRA analyst would typically ask an operator or trainer at the reference plant.

Teams should email a draft list of questions to the project coordinator by December 18, 2015. The project coordinator will arrange for a time slot between January 6-20, 2016, for each team

to conduct a phone interview with the operations SME. Follow-up questions after the phone interview will be answered by the testing team via email.

A.1.2.3 Perform HRA and Document Results

The HRA analysts will work in teams from their own worksites to analyze the five HFEs included in the testing. HRA analyst teams should use knowledge gained from the IDHEAS training along with the reference materials provided in this information package to perform their analyses. A template for documenting results and an example report have been provided in the information package.

A.1.2.4 Submit Results and Post-Analysis Questionnaire

Each HRA analyst team shall submit the following documentation by email to the project coordinator by February 12, 2016:

- Documentation of the HRA for each of the five HFEs
- Completed Post-Analysis Questionnaire (one per team)

A.1.2.5 Review Preliminary Evaluation of Results

After the HRA teams have submitted their final results, the project team will perform a preliminary evaluation of each team's results, including calculation of human error probabilities (HEPs) based on the team's selection of decision trees in the IDHEAS method. The HRA analyst teams will be asked to review the draft evaluation and provide comments.

A.1.2.6 Participate in Evaluation Workshop

The project team will take the results from each of the HRA analyst teams and perform an evaluation of the IDHEAS method guidance. The results of the evaluation will be shared with the analyst teams at an evaluation workshop (schedule TBD). The evaluation workshop will be an opportunity for the HRA analyst teams to share additional insights about their experiences with using the IDHEAS method.

A.1.3 Testing Schedule

Deadlines for HRA analyst teams are shown in bold.

Table A-2 Testing Schedule for HRA Analyst Teams

December 1-3, 2015	IDHEAS Testing Workshop
December 18, 2015	**Submit Initial List of Questions for Operations Subject Matter Expert**
January 6-20, 2016	Conduct Interviews with Operations Subject Matter Expert
February 12, 2016	**Submit Completed Testing Materials**
February 26, 2016	Receive preliminary evaluation of results for review

A.2 Scenario Descriptions

This section includes the descriptions of each of the three scenarios that were using in the study. The scenario descriptions are presented in the same format that was provided to the analyst teams.

A.2.1 Scenario 1: Steam Generator Tube Rupture

Plant technical information

4-loop Westinghouse pressurized water reactor (PWR)

Situation from start

- All participating crew members in control room (Shift Manager, Unit Supervisor, Shift Technical Advisor and two Reactor Operators)
- The plant is operating at 100%
- Core burnup is 19,000 MWD/MTU (EOL)

Steam generator tube rupture

While operating at power, a tube rupture occurs in steam generator (SG) C. The leak size is about 500 GPM at 100% power.

Definition of HFE 1: Failure to isolate the ruptured steam generator and control pressure below the SG PORV setpoint before SG PORV opening.

The time window to perform the required actions is estimated to be 3 hours.

The actions include:

- Isolate the ruptured SG (feedwater and main steam isolation valves closed).
- Maintain RCS pressure below the setpoint by cooling down the RCS (cooling the secondary by dumping steam and depressurizing the RCS).

Procedures that may be used

- 0POP05-EO-EO00 “Reactor Trip Or Safety Injection”
- 0POP05-EO-EO30 “Steam Generator Tube Rupture”
- 0POP05-EO-ES11 “SI Termination”

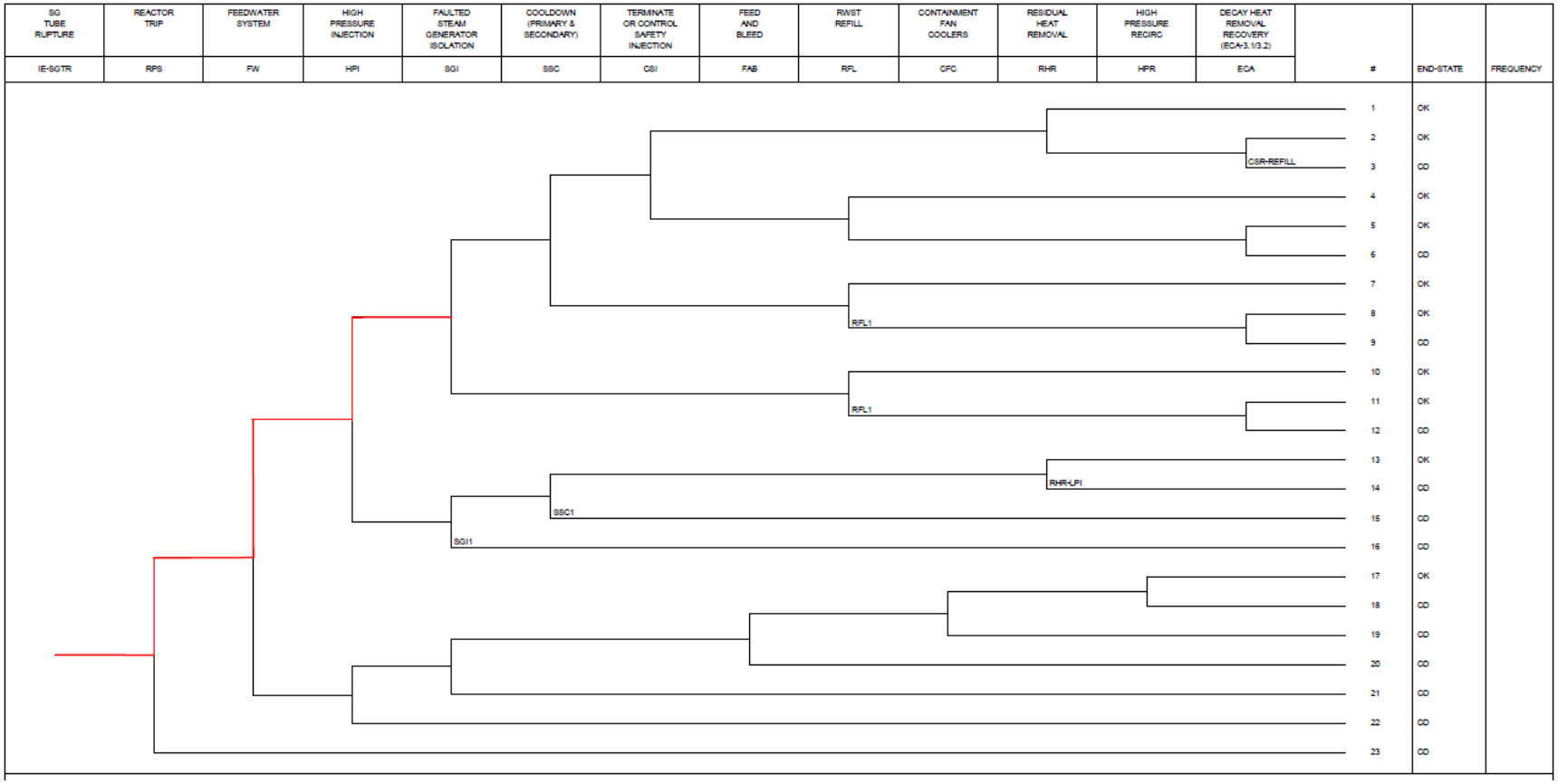


Figure 6-1 Steam Generator Tube Rupture Event Tree

A.2.2 Scenario 2: Total Loss of Feedwater (LOFW)

Plant technical information

- 4-loop Westinghouse pressurized water reactor (PWR)
- There are three main feedwater (MFW) pumps: 11, 12 and 13
- There are four auxiliary feedwater (AFW) pumps: 11, 12, 13 and 14. AFW pump 14 is turbine-driven and the other three motor-driven.

Situation from start

- The Shift Technical Advisor (STA) 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 (Shift Manager, Unit Supervisor, 2 Reactor Operators)
- The plant is operating at 100%
- Core burnup is 19,000 MWD/MTU (End of life)

Total loss of feedwater

During routine operation at power, MFW pump 11 is lost, and MFW pumps 12 and 13 trip within the next 10 seconds. The startup feedpump, which receives an auto start signal after the turbine driven feed pump, cannot be started. If the crew doesn't trip the reactor manually the reactor will trip on low SG level (20%).

At autostart, AFW pump 14 overspeeds and causes damage that cannot be repaired. AFW pump 11 has a seized shaft and trips and is therefore not available. AFW pump 13 starts but the shaft shears and no flow is indicated.

AFW pump 12 starts automatically and indicates full flow, but this flow will not reach (feed) the steam generators (SGs) because a manual recirculation valve is mis-positioned (it is open). There is no indication of the valve's position in the control room. Since there is no AFW flow to the SGs, the SG levels will go down rapidly before the reactor is tripped.

In reality, criteria to start FRH1 are met. But because of the indicated flow from AFW pump 12, the plant computer will not show a red path on the heatsink status tree.

The appropriate crew response to loss of heatsink is to enter the Response to Loss of Secondary Heat Sink procedure (FRH1) to start bleed and feed (B&F; *primary B&F,* with feed from safety injection and bleed through the pressurizer PORVs).

All attempts to establish AFW before the B&F initiation will fail.

Assuming the crew manually trips the reactor within approximately 30 - 45 seconds of the loss of feedwater, they will have approximately 45 minutes to initiate B&F before core damage (CD).

Definition of HFE 2: Failure to establish B&F within 45 minutes of the reactor trip, given that the crews initiate a manual reactor trip before an automatic reactor trip.

The actions to start B&F include:

- Actuate Safety Injection

- Open both of the PRZ PORVS

Procedures that may be used

- 0POP04-FW-0002 “Steam Generator Feed Pump Trip”
- 0POP05-EO-EO00 “Reactor Trip Or Safety Injection”
- 0POP05-EO-EO10 “Loss of Reactor or Secondary Coolant”
- 0POP05-EO-ES01 “Reactor Trip Response”
- 0POP05-EO-ES11 “SI Termination”
- 0POP05-EO-F003 “Heat Sink Critical Safety Function Status Tree”
- 0POP05-EO-FRH1 “Response to Loss of Secondary Heat Sink”

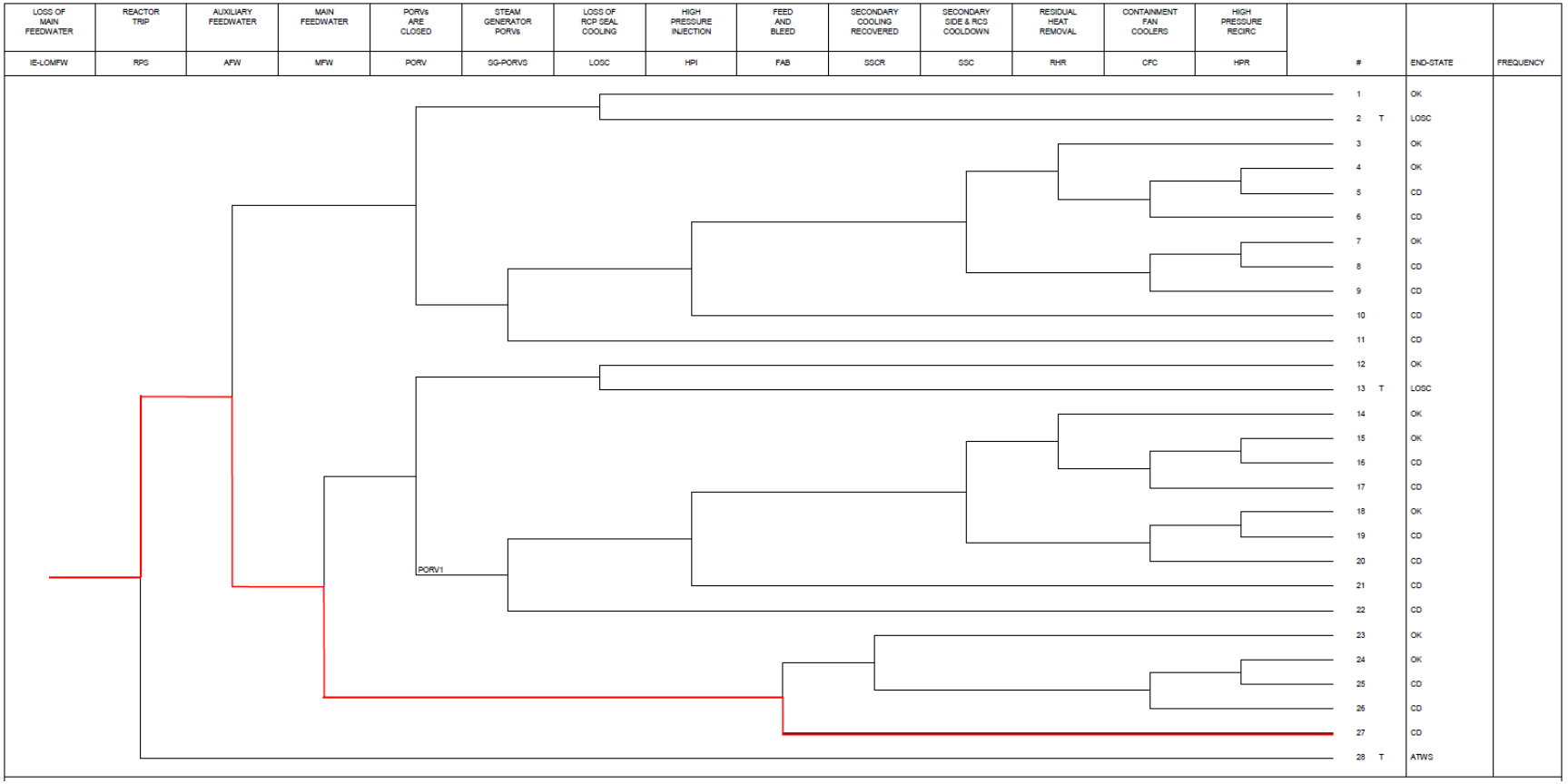


Figure 6-2 Loss of Main Feedwater Event Tree

A.2.3 Scenario 3: Electrical Fault Causes Fire and Subsequent Reactor Trip with Loss of Reactor Coolant Pump (RCP) Seal Injection and Cooling

This scenario is adapted from an actual event. Therefore, the HRA analyst is asked to perform an analysis of what could have happened, given the development of the plant status during the early phase of the event. HFE-3 and HFE-4 involve operator actions that either occurred or were actions that operators would have been expected to perform given available cues and procedures. HFE-5 is a key mitigation action required by operators to perform should a LOCA due to RCP seal failure occur, assuming the earlier operator actions had not been completed successfully.

Note that the operator actions would almost certainly be considered dependent. However, for this exercise, treat them as if they were independent, but try to take into account the context created by the scenario.

Plant technical information

- 3-loop Westinghouse pressurized water reactor (PWR)
- There are two main feedwater (FW) pumps: A and B
- There are three charging pumps: A, B and C
- There are three component cooling water (CCW) pumps: A, B and C

Situation from start

- The plant is operating in Mode 1 at approximately 100% power.
- The Shift Manager and Shift Technical Advisor are outside of the control room at a shift turnover meeting.
- CCW Pump C and Charging Pumps A and C are running.
- FW Pumps A and B are running.

Event overview

At 18:52, with the plant operating in Mode 1 at approximately 100% power, an electrical feeder cable failure caused an arc flash and fire on a non-vital electrical bus. The electrical bus failed to isolate due to a breaker failure, and the fault persisted much longer than design expectations. The effects were widespread throughout the electrical systems. The electrical isolations and automatic repowering also created time sequences that caused inadvertent equipment actuation and damage. The fault condition reduced voltage to Reactor Coolant Pump (RCP) B, causing an automatic reactor trip on Reactor Coolant System (RCS) loop low flow. Pressurizer level and pressure decreased due to RCS cooldown, resulting in an automatic safety injection (SI). Plant response was further complicated by multiple equipment malfunctions.

Loss of RCP seal injection and cooling

Within the first minute of the initiating event, RCP seal cooling (via Component Cooling Water (CCW)) is lost due to the closing of Flow Control Valve (FCV) 626, the component cooling water thermal barrier outlet isolation valve. FCV-626 closed due to an inaccurate high-flow signal when the flow sensor lost power during electrical realignments resulting from the fault.

Approximately 27 minutes into the event, Chemical and Volume Control (CVC) Valve 310A fails open. When CVC-310A fails open the charging flow is diverted from the RCP seals to the RCS

and RCP seal injection becomes inadequate (there is some injection flow, but it is inadequate to fulfill its safety function). As a result, the RCP seals begin to heat up and purge volume begins to empty.

With both RCP seal cooling from CCW unavailable and seal injection inadequate, the appropriate crew response would be to restore seal cooling from CCW to the RCP thermal barrier heat exchangers.

Definition of HFE 3: Failure to restore CCW to the RCP thermal barrier heat exchangers by re-opening FCV-626.

For successful recovery, operators would have to re-open FCV-626 from the control room before voiding within the RCPs occurs. Based on Westinghouse calculations, the RCP seals will experience voiding conditions approximately 19 minutes after all RCP seal cooling and injection are lost.

Definition of HFE 4: Failure to trip the RCPs during a loss of all seal cooling and injection.

If FCV-626 is not opened in time or cannot be opened, operators would need to trip the running RCPs prior to failure of the seals (HFE-4). RCP Pump B was tripped due to the loss of Bus 4 during the initial electrical fault. RCPs A and C remained running.

Operators have approximately 19 minutes from when seal cooling and injection are lost to trip the running RCPs and avoid catastrophic seal failure (large enough to be equivalent to a small loss of coolant accident).

Small loss of coolant accident (SLOCA)

If operators fail to stop the RCPs and restore cooling prior to the seals being fully challenged, the seals will fail at the maximum leakage rate of 480 gpm per RCP. The RCP seal failure will lead to a SLOCA. Pressurizer level will decrease, the pressurizer low pressure alarm will annunciate, and containment spray will activate with radiation alarms. The expected crew response would be to initiate a cooldown and depressurization of the RCS to allow for the plant to be placed in shutdown cooling (SDC) using the residual heat removal (RHR) system.

Definition of HFE 5: Failure to depressurize the RCS during a small loss of coolant accident (SLOCA).

To initiate a successful RCS cooldown, operators must depressurize the RCS by using the pressurizer PORVs or pressurizer sprays. The operators must also initiate a secondary side cooldown using the steam generator atmospheric relief valves or the turbine bypass valves to remove the decay heat and depressurize the RCS.

Operators would have at least two hours to initiate the RCS cooldown and depressurization prior to depletion of the RWST inventory during an SLOCA caused by failure of RCP seals.

Procedures that may be used

- EOP Path-1 “Emergency Procedure Flow Path”
- End Path Procedure (EPP) 4, “Reactor Trip Response”
- APP-001-D1 “Annunciator Panel Procedure - RCP THERM BAR COOL WTR LO FLOW”

- EPP-7 “SI Termination”
- EPP-8 “Post LOCA Cooldown and Depressurization”
- EPP-Foldout A
- AOP-18 “Abnormal RCP Condition”

Sequence of key events

18:40 Pre-event plant status was 100% power, CCW C Pump is running, and Charging Pumps A and C are running. No safety equipment was out of service for testing or maintenance.

18:52 an electrical fault and fire occurs on the cable entering 4kV Bus 5. Breaker 24 in 4kV Bus 4 should have isolated the fault in 0.9 seconds but remained closed. This allows the fault to last long enough to lower the bus voltage and decrease flow in RCP B below the low flow trip setpoint of the Reactor Protection System, resulting in an automatic reactor trip.

Due to electrical realignments, Charging Pump A, Charging Pump C (RCP seal injection lost) and CCW Pump C are lost. CCW Pump B starts on loss of Instrument Bus 4, CCW Pump C restarts on the sequencer and FCV-626 (thermal barrier outlet isolation flow control valve) closes stopping flow from the thermal barrier heat exchangers. Therefore, RCP seal cooling from the thermal barrier heat exchangers is lost. The RCP thermal barrier cooling water low flow alarm annunciates.

Operators respond to the reactor trip by entering EOP Path-1, Emergency Procedure Flow Path, determine that no SI is required and transition to End Path Procedure (EPP) 4, Reactor Trip Response. During the first 30 minutes of the event, the reactor coolant system cooldown rate was approximately 200°F/hr.

18:53 Operators start Charging Pumps B and C per Path-1; RCP seal injection is restored.

18:54 Pressurizer level = 14% and letdown system isolates.

The Shift Manager and STA arrive in the main control room from a shift turnover meeting and report the fire at Bus 5. The BOP operator implements AOP-41, Response to a Fire Event, and remains dedicated to this procedure for approximately 40 minutes.

18:58 Pressurizer level is low out-of-sight.

The fire in Bus 5 is reported extinguished, but reflashes several times.

19:00 Due to cooldown through the MSR drains, pressurizer level and pressure decrease to the pressurizer low pressure SI setpoint. The reactor automatically safety injects as designed. Charging Pump C trips in response to SI signal which was the normal expected response based on Bus E2 powered from EDG B and Bus E1 powered from normal power. Letdown automatically isolates on Phase-A Containment Isolation.

VCT level decreases to setpoint for auto transfer to the Refueling Water Storage Tank RWST. This automatic transfer does not occur, hence VCT level continues to decrease. No attempts are made to shut the MSIVs and stop the cooldown and depressurization.

Charging Pump B remained running at 18 gpm. This is the only source injecting water to the core at this time, and it is draining down the VCT further. Operators re-enter Path-1.

19:01 charging flow at 18 gpm and slowly decreasing.

19:03 SI systems begin to inject based on RCS pressure dropping below shutoff head of the pumps.

19:12 VCT at lowest indicated level during the event (approximately 2–3 inches).

19:13 SI systems no longer injecting to RCS based on pressure at shutoff head for the pumps.

19:19 charging flow automatically increased to 25 gpm due to the isolation of instrument air to containment resulting in "bleed-off" of air, causing CVC-310A (Charging to Loop 1) valve in the charging system to fail open. The opening of CVC- 310A diverts charging flow from the RCP seals to the RCS causing the RCP seal injection to be inadequate.

19:24 RCP B Bearing high temperature alarm received. This was the first indication that the RCP seals are being challenged.

19:25 MSIVs shut due to a valid signal from the low Tave coincident with a loss of Instrument Bus 3 (caused by operator error during another manipulation); this effectively terminated the uncontrolled RCS cooldown.

19:27 Instrument Bus 3 power is restored.

19:30 RCP A Bearing high temperature alarm received.

19:33 RCP B Seal #1 leak-off high temperature alarm received; RCP C Bearing high temperature alarm received.

LOSS OF MAIN FEEDWATER	REACTOR TRIP	AUXILIARY FEEDWATER AVAILABLE		PORV/SRVs ARE CLOSED	LOSS OF SEAL COOLING		HIGH PRESSURE INJECTION	FEED AND BLEED	SECONDARY SIDE COOLING RECOVERED	COOLDOWN (PRIMARY & SECONDARY)	RESIDUAL HEAT REMOVAL	HPR PRESSURE RECIRC	#	End State (Phase - CD)
IE-LOMFW	RPS	AFW	FTF-LOOP-RECOVERY	PORV	LOSC	FTF-LOSC	HPI	FAB	SSCR	SSC	RHR	HPR		

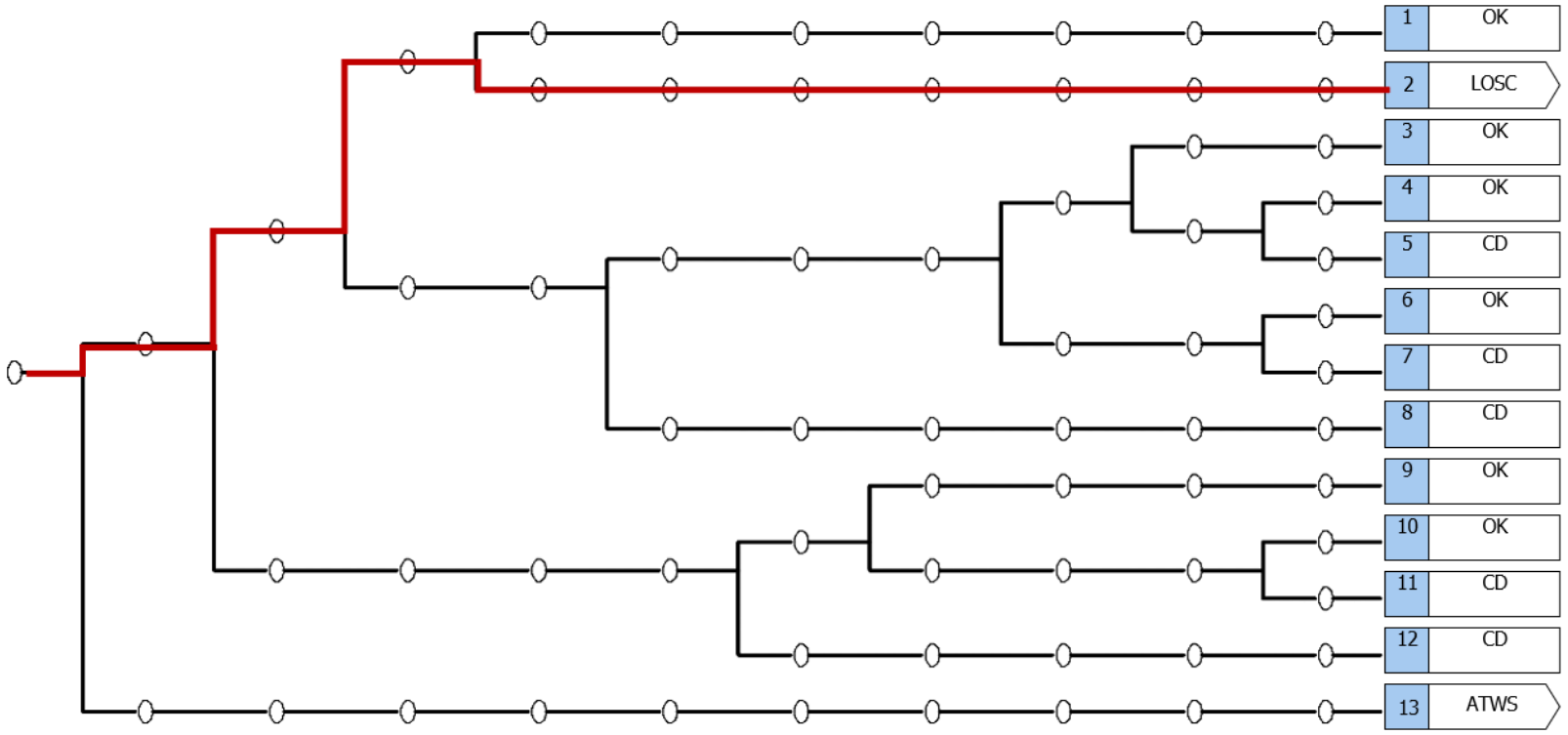


Figure 6-3 Loss of Main Feedwater Event Tree

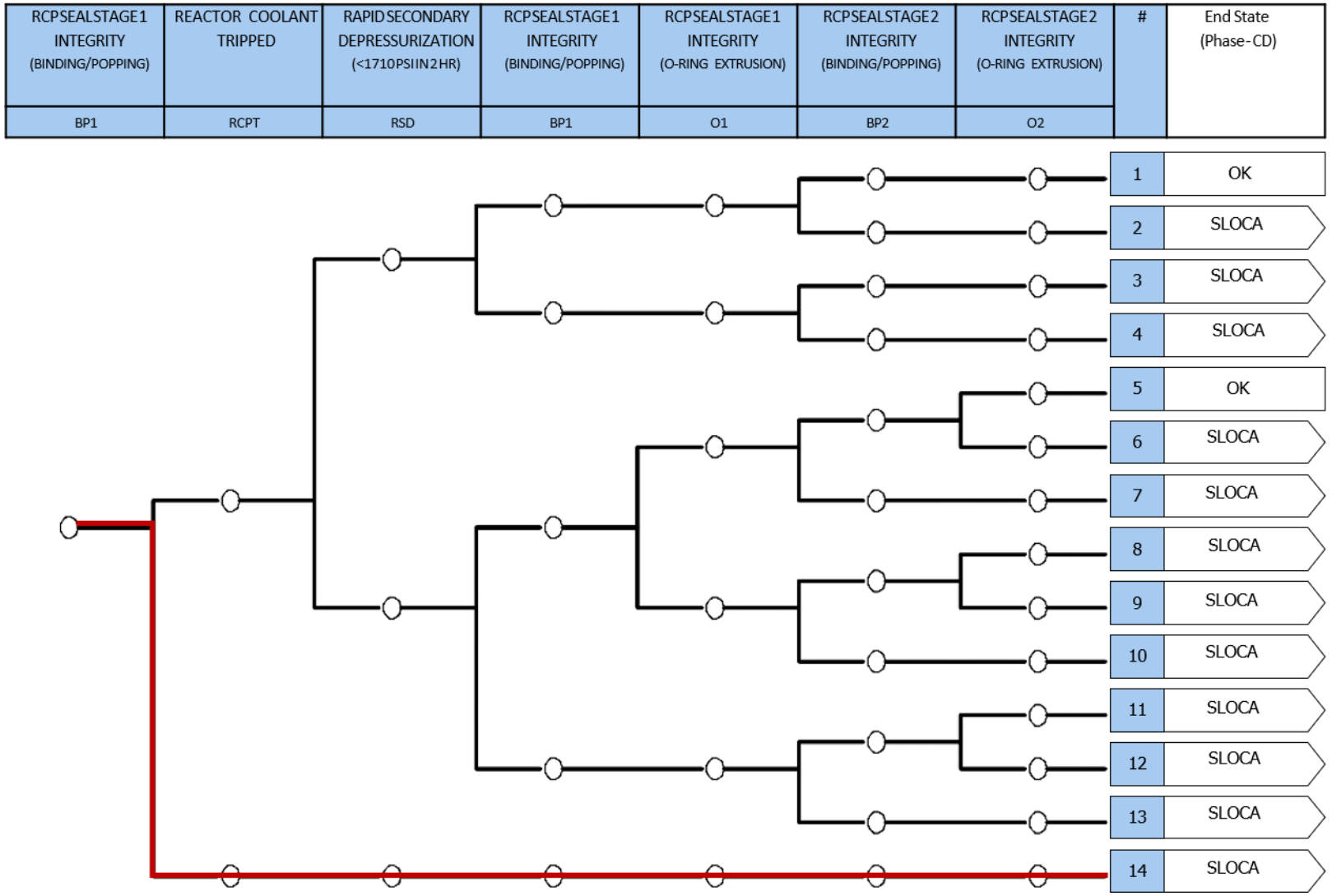


Figure 6-4 Loss of Seal Cooling Event Tree

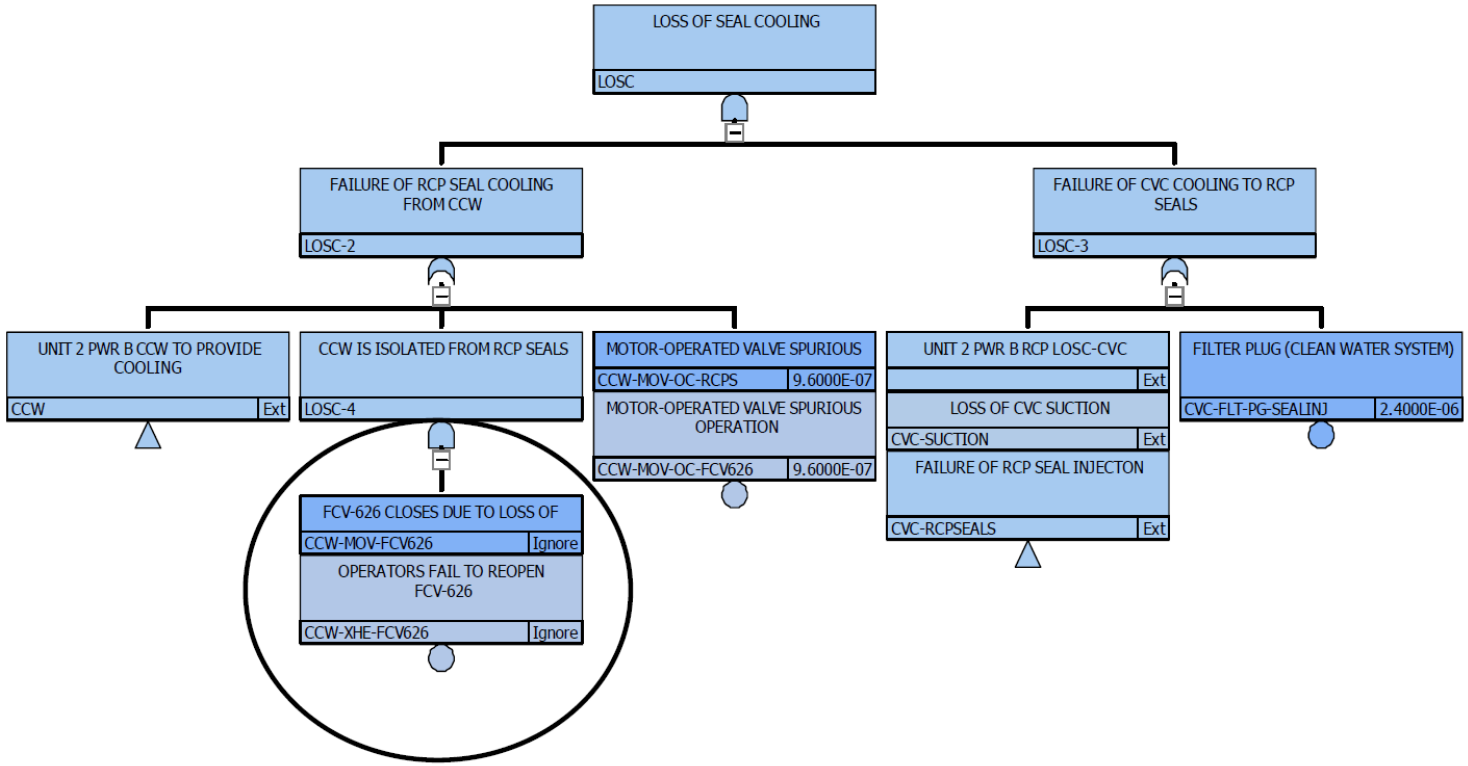


Figure 6-5 Loss of Seal Cooling Fault Tree

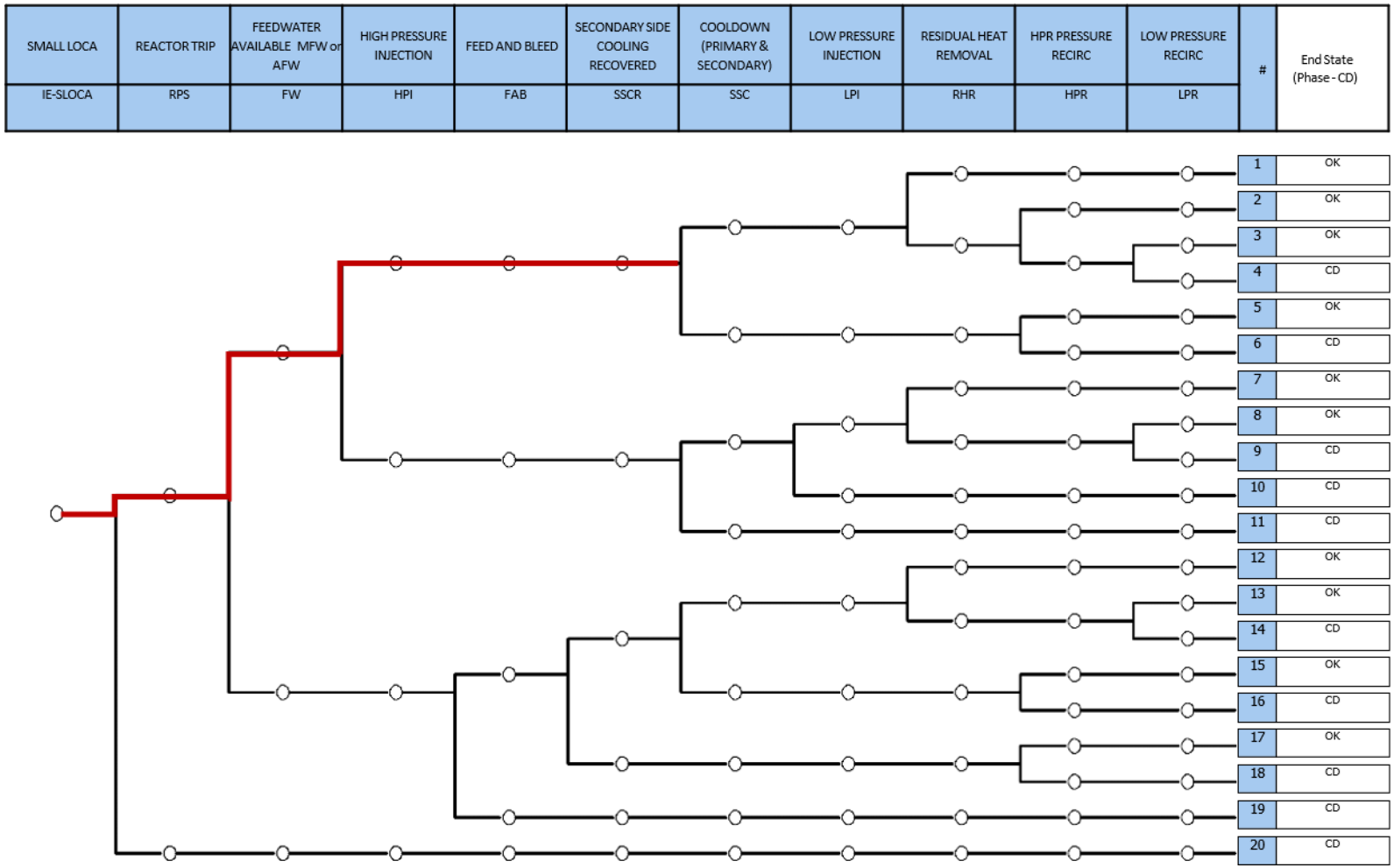


Figure 6-6 Small Loss of Coolant Accident Event Tree

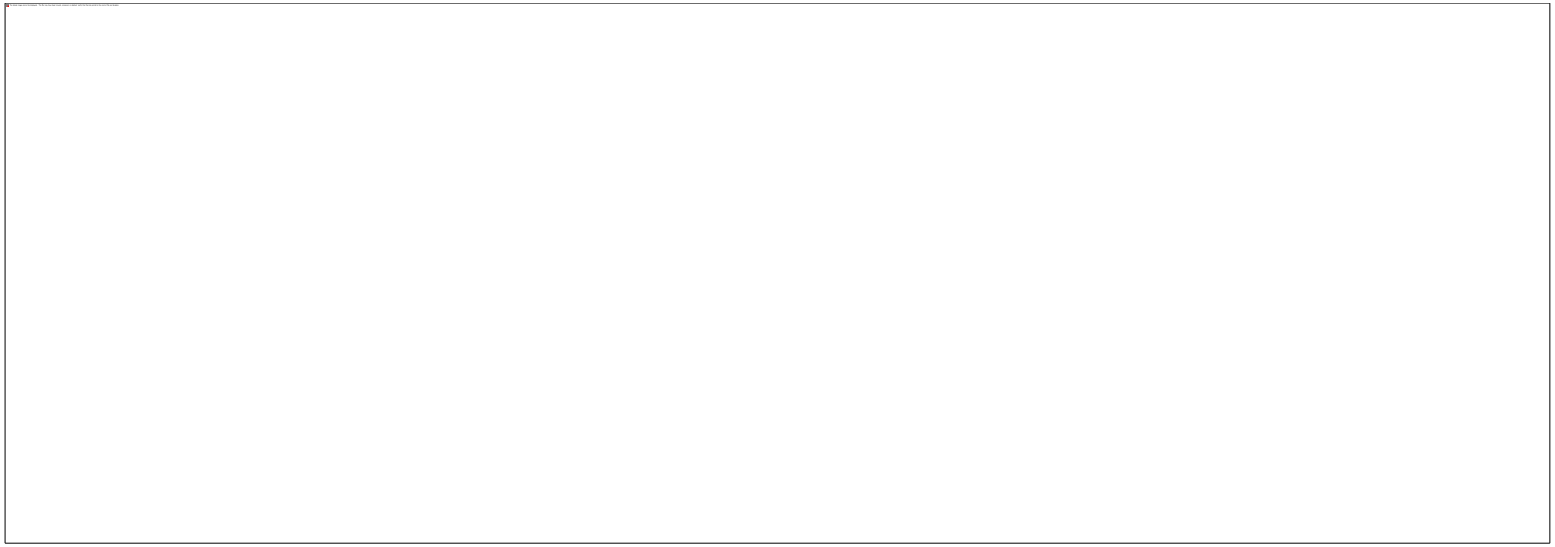


Figure 6-7 RCS Cooldown Fault Tree

A.3 Post-Analysis Questionnaire

This section presents the questionnaire that analysts were asked to complete after they completed their analysis of each of the human failure events using IDHEAS AT-POWER.

Team Member Names: Click here to enter text.

SECTION 1: This section asks about each HFE that you analyzed. Answer these questions after you complete the analysis for each HFE.

HFE 1

1. How much time did it take your team to perform the analysis for this HFE? (Please include all time that each analyst spent working on the HFE)
   Click here to enter text.

2. How difficult are the human actions associated with this HFE? (Where extremely easy indicates that a crew is highly likely to succeed, and extremely difficult indicates that a crew is highly likely to fail)

EXTREMELY EASY	VERY EASY	SOMEWHAT EASY	ABOUT AVERAGE	SOMEWHAT DIFFICULT	VERY DIFFICULT	EXTREMELY DIFFICULT
1	2	3	4	5	6	7
☐	☐	☐	☐	☐	☐	☐

   a. Why should the actions be easy or difficult?
      Click here to enter text.

3. Based on your analysis, what human error probability (HEP) would you predict for this HFE?

HEP	Click here to enter text.

4. In this scenario, what do you think were the main contributors to human error?
   Click here to enter text.

5. Do you think there were other failure modes or influencing factors that were important for this HFE, but were not well captured or covered by the IDHEAS guidance?
   Click here to enter text.

6. When choosing CFM decision tree paths for this HFE, were there any branch points where you had difficulty determining which path to choose? If yes, please describe.
   Click here to enter text.

HFE 2

1. How much time did it take your team to perform the analysis for this HFE? (Please include all time that each analyst spent working on the HFE)
   Click here to enter text.

2. How difficult are the human actions associated with this HFE? (Where extremely easy indicates that a crew is highly likely to succeed, and extremely difficult indicates that a crew is highly likely to fail)

EXTREMELY EASY	VERY EASY	SOMEWHAT EASY	ABOUT AVERAGE	SOMEWHAT DIFFICULT	VERY DIFFICULT	EXTREMELY DIFFICULT
1	2	3	4	5	6	7
☐	☐	☐	☐	☐	☐	☐

a. Why should the actions be easy or difficult?
Click here to enter text.

3. Based on your analysis, what human error probability (HEP) would you predict for this HFE?

HEP	Click here to enter text.

4. In this scenario, what do you think were the main contributors to human error?
Click here to enter text.

5. Do you think there were other failure modes or influencing factors that were important for this HFE, but were not well captured or covered by the IDHEAS guidance?
Click here to enter text.

6. When choosing CFM decision tree paths for this HFE, were there any branch points where you had difficulty determining which path to choose? If yes, please describe.
Click here to enter text.

HFE 3

1. How much time did it take your team to perform the analysis for this HFE? (Please include all time that each analyst spent working on the HFE)
Click here to enter text.

2. How difficult are the human actions associated with this HFE? (Where extremely easy indicates that a crew is highly likely to succeed, and extremely difficult indicates that a crew is highly likely to fail)

EXTREMELY EASY	VERY EASY	SOMEWHAT EASY	ABOUT AVERAGE	SOMEWHAT DIFFICULT	VERY DIFFICULT	EXTREMELY DIFFICULT
1	2	3	4	5	6	7
☐	☐	☐	☐	☐	☐	☐

a. Why should the actions be easy or difficult?
Click here to enter text.

3. Based on your analysis, what human error probability (HEP) would you predict for this HFE?

HEP	Click here to enter text.

4. In this scenario, what do you think were the main contributors to human error?
Click here to enter text.

5. Do you think there were other failure modes or influencing factors that were important for this HFE, but were not well captured or covered by the IDHEAS guidance?
Click here to enter text.

6. When choosing CFM decision tree paths for this HFE, were there any branch points where you had difficulty determining which path to choose? If yes, please describe.
   Click here to enter text.

HFE 4

1. How much time did it take your team to perform the analysis for this HFE? (Please include all time that each analyst spent working on the HFE)
   Click here to enter text.

2. How difficult are the human actions associated with this HFE? (Where extremely easy indicates that a crew is highly likely to succeed, and extremely difficult indicates that a crew is highly likely to fail)

EXTREMELY EASY	VERY EASY	SOMEWHAT EASY	ABOUT AVERAGE	SOMEWHAT DIFFICULT	VERY DIFFICULT	EXTREMELY DIFFICULT
1	2	3	4	5	6	7
☐	☐	☐	☐	☐	☐	☐

   a. Why should the actions be easy or difficult?
      Click here to enter text.

3. Based on your analysis, what human error probability (HEP) would you predict for this HFE?

HEP	Click here to enter text.

4. In this scenario, what do you think were the main contributors to human error?
   Click here to enter text.

5. Do you think there were other failure modes or influencing factors that were important for this HFE, but were not well captured or covered by the IDHEAS guidance?
   Click here to enter text.

6. When choosing CFM decision tree paths for this HFE, were there any branch points where you had difficulty determining which path to choose? If yes, please describe.
   Click here to enter text.

HFE 5

1. How much time did it take your team to perform the analysis for this HFE? (Please include all time that each analyst spent working on the HFE)
   Click here to enter text.

2. How difficult are the human actions associated with this HFE? (Where extremely easy indicates that a crew is highly likely to succeed, and extremely difficult indicates that a crew is highly likely to fail)

EXTREMELY EASY	VERY EASY	SOMEWHAT EASY	ABOUT AVERAGE	SOMEWHAT DIFFICULT	VERY DIFFICULT	EXTREMELY DIFFICULT
1	2	3	4	5	6	7
☐	☐	☐	☐	☐	☐	☐

   a. Why should the actions be easy or difficult?
      Click here to enter text.

3. Based on your analysis, what human error probability (HEP) would you predict for this HFE?

HEP	Click here to enter text.

4. In this scenario, what do you think were the main contributors to human error?
   Click here to enter text.

5. Do you think there were other failure modes or influencing factors that were important for this HFE, but were not well captured or covered by the IDHEAS guidance?
   Click here to enter text.

6. When choosing CFM decision tree paths for this HFE, were there any branch points where you had difficulty determining which path to choose? If yes, please describe.
   Click here to enter text.

SECTION 2: This section asks about your overall experience using the IDHEAS method. Answer these questions after you analyze all of the HFEs.

1. Please rank each HFE in terms of overall difficulty for an operator to perform. (Where 1 is the least difficult HFE, and 5 is the most difficult HFE)

1 - LEAST DIFFICULT	Click here to enter text.
2	Click here to enter text.
3	Click here to enter text.
4	Click here to enter text.
5 - MOST DIFFICULT	Click here to enter text.

2. On average, how much time do you think it would take you to analyze an HFE using IDHEAS, after you had gained some experience with the method?
   Click here to enter text.

3. To what extent was IDHEAS easy to learn? (check one)

EXTREMELY EASY	VERY EASY	SOMEWHAT EASY	ABOUT AVERAGE	SOMEWHAT DIFFICULT	VERY DIFFICULT	EXTREMELY DIFFICULT
1	2	3	4	5	6	7
☐	☐	☐	☐	☐	☐	☐

4. To what extent was IDHEAS easy to use? (check one)

EXTREMELY EASY	VERY EASY	SOMEWHAT EASY	ABOUT AVERAGE	SOMEWHAT DIFFICULT	VERY DIFFICULT	EXTREMELY DIFFICULT
1	2	3	4	5	6	7
☐	☐	☐	☐	☐	☐	☐

5. To what extent was the IDHEAS guidance clear? (check one)

EXTREMELY CLEAR	VERY CLEAR	SOMEWHAT CLEAR	NEITHER CLEAR NOR UNCLEAR	SOMEWHAT UNCLEAR	VERY UNCLEAR	EXTREMELY UNCLEAR
1	2	3	4	5	6	7
☐	☐	☐	☐	☐	☐	☐

6. Were there parts of the IDHEAS method where you felt the guidance was unclear? If yes, please describe.
   Click here to enter text.

7. How does the IDHEAS method compare to other HRA methods you have used? (e.g., ease of use, comprehensiveness, documentation of results)
   Click here to enter text.

   a. Please indicate what other HRA methods you are comparing IDHEAS to.
      Click here to enter text.

8. Would you use IDHEAS in place of other HRA methods? (check one)

Yes	☐	**No**	☐

   a. If yes, when would you be most likely to use IDHEAS? If no, why not?
      Click here to enter text.

9. Based on your experience, please list positive aspects of the IDHEAS method.
   Click here to enter text.

10. Based on your experience, list areas for improvement in the IDHEAS method and its guidance.
    Click here to enter text.

11. Please include any additional comments about your experience using IDHEAS.
    Click here to enter text.

A.4 Documentation Template

This section presents the template that was provided to the analysts for documenting their analysis results.

Please use this template to assist in documenting your analysis of each HFE. Instructions appear in blue italic font. The instructions provide recommendations and should not be considered all-inclusive; you are encouraged to document all information relevant to your analysis. Refer to the example IDHEAS report for a demonstration of how to use the template and associated tables.

1. PRA Scenario Description, Expected Operator Response and HFE Definition

This section should include the following information:

- *Initial plant conditions*
- *Accident sequence (plant system and equipment response)*
- *Functional description of required operator response (e.g., perform feed and bleed, depressurize reactor to allow low pressure injection, restore cooling to RCP seals)*
- *Functional success criterion (e.g., achieve feed and bleed prior to core damage)*
- *Consequence of failure*
- *Definition of the HFE*

2. Crew Response Diagram (CRD) and Task Analysis

Include a picture of the CRD, summary of the development of the CRD, and description of each node on the CRD, including, but not limited to:

- *Description of the procedural path for successful crew response*
- *Justification of the chosen success path, taking into account:*
  - *Availability of information needed for success*
  - *Manpower available*
  - *Timing of key cues/indications, relative to time needed to proceed through the procedures and time available for successful response*
  - *Understanding of priorities for responses (e.g., EOPs over APPs may be important when there are competing demands on the crews)*
- *Identification of recovery opportunities, taking into account:*
  - *Availability of information needed to effect recovery*
  - *Manpower available*
  - *Timing of key cues/indications relative to time taken to proceed through the procedures and time available for successful response*
- *Assumptions made in the construction of the CRD*

Include documentation of the task analysis for each CRD node, including:

- *Decomposition of CRD nodes into critical tasks*
- *Characterization of critical tasks and associated activities that are required to achieve the critical tasks*
- *Additional information regarding task context, timing, workload, etc. that may impact success or failure of the critical task*

Use the "Task Analysis Table" to assist in summarizing the task analysis and identification of critical tasks. Note that each node on the success path may have one or more critical tasks. Recovery nodes and nodes included for information only do not need to be documented in a Task Analysis Table, but should be included in the narrative description of the CRD.

Table A-3 Task Analysis Table

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information

3. Timeline

Include a picture and description of the timeline, including, but not limited to:

- *Description of each time point illustrated on the timeline (e.g., cues, indications, steps or transition points in the procedural path)*
- *Information source for identification of each time point*
- *Assumptions made in the construction of the timeline*

Include discussion of feasibility of successful crew response.

4. Evaluation of Crew Failure Modes (CFMs) and Decision Trees

Evaluate each critical task to determine the applicable Crew Failure Modes (CFMs). *Complete a "CFM Selection Table" for each critical task. The required activities for the critical task documented in the Task Analysis Table should assist you in evaluating whether the critical task involves activities in the Status Assessment, Response Planning, or Execution phase of crew response. Refer to the IDHEAS reference material, Attachment 1: CFMs and decision trees, for guidance on choosing CFMs and deciding between branch points on the CFM decision trees. Remember to provide a justification for each CFM.*

Table A-4 CFM Selection Table

CRD Node		
Critical Task		
CFMs	**Applicable? (Yes/No)**	**Justification**
AP-1: Key Alarm not Attended to		

AP-2: Misread or Skip Critical Step(s) in Procedure		
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		
RP-1: Misinterpret Procedures		
RP-2: Choose Inappropriate Strategy		
E-1: Delay Implementation		
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency		
E-3: Fail to Initiate Execution		
E-4: Fail to Correctly Execute Response (Simple Task)		
E-5: Fail to Correctly Execute Response (Complex Task)		

For each CFM that is identified as applicable, evaluate the CFM decision tree and determine the relevant crew failure scenario based on the decision tree branches. *Use the "Decision Tree Tables" to document your justification for each branch path selection based on your assessment of the performance influencing factors (PIFs) included in the tree (see additional "Decision Tree Tables" at the end of this document).*

Table A-5 Decision Tree Table for SA-3

SA-3: Critical Data Misperceived		
PIF	**Assessment**	**Justification**
HSI/Environment	*Poor or Good*	
Workload	*High or Low*	
Training	*Poor or Good*	
Recovery Potential	*No or Yes*	
Crew Failure Scenario #		*insert number from decision tree based on branch path selected*

5. Summary of Analysis

Provide a summary narrative of your analysis *(1-3 paragraph summary of the HFE and insights from the analysis). This should be written as a way to bring all the qualitative information together as a "sanity check" of the analysis and ensure that the "big picture" did not*

get lost. This narrative can also include a summary of assumptions made or uncertainties identified in the analysis.

Complete the "HEP Calculation Table." *This table provides summary information to aid in quantification of the HEP. The table should include all critical tasks, CFMs that were identified as applicable for each critical task, and the associated crew failure scenario that was selected from the CFM Decision Tree. Note that the HEP column of this table should be left blank. HEP calculations will be performed by the project team based on the selected decision tree branch points. Add or delete rows as needed.*

Table A-6 HEP Calculation Table

CRD Node #	Critical Task #	CFM	Crew Failure Scenario #	HEP
Total HEP:				

APPENDIX B
IDHEAS AT-POWER HUMAN ERROR PROBABILITIES

This appendix presents the mean human error probabilities (HEPs) that correspond to the crew failure mode decision trees used in the testing of IDHEAS AT-POWER. Note that the analyst teams were not provided with these human error probabilities until after they had submitted their analysis results. This was done to reduce the likelihood that the analysts' choice of crew failure scenario on a decision tree would be influenced by the human error probability associated with that failure scenario.

Table B-1 AP-1: Key Alarm Not Attended To

Crew Failure Scenario	Performance-Influencing Factors			Mean HEP
	Distraction	HSI	Perceived Urgency	
1	High	Poor	Low	2.5E-01
2	High	Poor	High	9.8E-02
3	High	Good	Low	6.5E-02
4	High	Good	High	4.4E-03
5	Low	Poor	Low	7.3E-03
6	Low	Poor	High	9.6E-04
7	Low	Good		2.4E-05

Table B-2 AP-2: Misread or Skip Step in Procedure

Crew Failure Scenario	Performance-Influencing Factors				Mean HEP
	Workload	Procedure	Compensatory Factors	Recovery Potential	
1	High	Complex	Not present	No	9.4E-02
2	High	Complex	Not present	Yes	1.3E-02
3	High	Complex	Present	No	1.9E-02
4	High	Complex	Present	Yes	2.7E-03
5	High	Simple	Not present	No	1.3E-02
6	High	Simple	Not present	Yes	1.9E-03
7	High	Simple	Present	No	1.0E-03
8	High	Simple	Present	Yes	1.5E-04
9	Low	Complex	Not present	No	3.6E-02
10	Low	Complex	Not present	Yes	5.1E-03
11	Low	Complex	Present	No	1.3E-03
12	Low	Complex	Present	Yes	9.7E-05
13	Low	Simple		No	8.2E-04
14	Low	Simple		Yes	1.2E-04

Table B-3 SA-1: Data Misleading or Not Available

Crew Failure Scenario	Performance-Influencing Factors				Mean HEP
	Alternate Source of Information	Information Obviously Incorrect	Guidance to Seek Confirmatory Data	Distraction	
1	No				
2	Yes	No	No	High	3.6E-01
3	Yes	No	No	Low	3.2E-01
4	Yes	No	Yes	High	1.5E-01
5	Yes	No	Yes	Low	9.6E-03
6	Yes	Yes	No	High	1.1E-01
7	Yes	Yes	No	Low	1.2E-02
8	Yes	Yes	Yes	High	3.1E-02
9	Yes	Yes	Yes	Low	3.4E-03

Table B-4 SA-2: Wrong Data Source Attended To

Crew Failure Scenario	Performance-Influencing Factors				Mean HEP
	HSI	Workload	Familiarity with Data Source	Recovery	
1	Poor	High	Poor	No	8.2E-02
2	Poor	High	Poor	Yes	3.9E-02
3	Poor	High	Good	No	2.5E-02
4	Poor	High	Good	Yes	4.2E-03
5	Poor	Low	Poor	No	3.3E-02
6	Poor	Low	Poor	Yes	5.4E-03
7	Poor	Low	Good	No	7.2E-03
8	Poor	Low	Good	Yes	1.2E-03
9	Good	High	Poor	No	6.2E-03
10	Good	High	Poor	Yes	8.3E-04
11	Good	High	Good	No	2.0E-03
12	Good	High	Good	Yes	3.2E-04
13	Good	Low	Poor	No	2.0E-03
14	Good	Low	Poor	Yes	3.2E-04
15	Good	Low	Good	No	5.2E-04
16	Good	Low	Good	Yes	5.2E-05

Table B-5 SA-3: Critical Data Misperceived

Crew Failure Scenario	Performance-Influencing Factors				Mean HEP
	HSI	Workload	Training	Recovery	
1	Poor	High	Poor	No	5.6E-01
2	Poor	High	Poor	Yes	5.7E-02
3	Poor	High	Good	No	1.1E-02
4	Poor	High	Good	Yes	5.7E-03
5	Poor	Low	Poor	No	6.5E-03

6	Poor	Low	Poor	Yes	1.3E-03
7	Poor	Low	Good	No	1.3E-04
8	Poor	Low	Good	Yes	2.6E-05
9	Good	High	Poor	No	5.7E-03
10	Good	High	Poor	Yes	1.3E-04
11	Good	High	Good	No	1.6E-04
12	Good	High	Good	Yes	3.4E-05
13	Good	Low	Poor	No	1.3E-04
14	Good	Low	Poor	Yes	1.3E-05
15	Good	Low	Good	No	1.3E-05
16	Good	Low	Good	Yes	1.3E-05

Table B-6 SA-4: Critical Data Dismissed/Discounted

Crew Failure Scenario	Performance-Influencing Factors					Mean HEP
	Valid Alternative Scenario	Inappropriate Bias	Indications Reliable	Confirmatory Information	Recovery potential	
1	Yes	Formed	No	No	No	4.9E-01
2	Yes	Formed	No	No	Yes	5.0E-02
3	Yes	Formed	No	Yes	No	4.5E-02
4	Yes	Formed	No	Yes	Yes	4.5E-03
5	Yes	Formed	Yes	No	No	2.5E-01
6	Yes	Formed	Yes	No	Yes	2.5E-02
7	Yes	Formed	Yes	Yes	No	2.5E-02
8	Yes	Formed	Yes	Yes	Yes	2.5E-03
9	Yes	Not Formed	No	No	No	3.3E-03
10	Yes	Not Formed	No	No	Yes	3.3E-04
11	Yes	Not Formed	No	Yes	No	3.1E-04
12	Yes	Not Formed	No	Yes	Yes	3.1E-05
13	Yes	Not Formed	Yes	No	No	1.6E-03
14	Yes	Not Formed	Yes	No	Yes	1.6E-04
15	Yes	Not Formed	Yes	Yes		1.3E-05
16	No					

Table B-7 SA-5: Premature Termination of Critical Data Collection

Crew Failure Scenario	Performance-Influencing Factors					Mean HEP
	Viable plant status believable	Expectations or Biases	Workload	HSI	Recovery Potential	
1	Yes	Formed	High	Poor	No	1.1E-01
2	Yes	Formed	High	Poor	Yes	1.3E-02
3	Yes	Formed	High	Good	No	5.1E-02
4	Yes	Formed	High	Good	Yes	5.1E-03
5	Yes	Formed	Low	Poor	No	7.6E-02
6	Yes	Formed	Low	Poor	Yes	7.6E-03
7	Yes	Formed	Low	Good	No	8.2E-03
8	Yes	Formed	Low	Good	Yes	8.2E-04

9	Yes	Not Formed	High	Poor	No	1.3E-02
10	Yes	Not Formed	High	Poor	Yes	1.3E-03
11	Yes	Not Formed	High	Good	No	4.1E-03
12	Yes	Not Formed	High	Good	Yes	4.1E-04
13	Yes	Not Formed	Low	Poor	No	4.2E-03
14	Yes	Not Formed	Low	Poor	Yes	4.2E-04
15	Yes	Not Formed	Low	Good	No	3.5E-04
16	Yes	Not Formed	Low	Good	Yes	3.5E-05
17	No					

Table B-8 RP-1: Misinterpret Procedure

Crew Failure Scenario	Performance-Influencing Factors				Mean HEP
	Procedure Open to Misinterpretation	Workload	Training	Recovery Potential	
1	Yes	High	Less than adequate	No	2.3E-01
2	Yes	High	Less than adequate	Yes	3.3E-02
3	Yes	High	Good	No	7.3E-02
4	Yes	High	Good	Yes	5.3E-03
5	Yes	Low	Less than adequate	No	7.3E-02
6	Yes	Low	Less than adequate	Yes	3.6E-03
7	Yes	Low	Good		1.6E-04
8	No				

Table B-9 RP-2: Choose Inappropriate Strategy

Crew Failure Scenario	Performance-Influencing Factors			Mean HEP
	Preference for Correct Strategy	Advantage to The Correct Strategy	Recovery Potential	
1	Low	No	No	5.2E-01
2	Low	No	Yes	8.2E-02
3	Low	Yes	No	1.4E-01
4	Low	Yes	Yes	1.4E-02
5	High	No	No	3.3E-02
6	High	No	Yes	3.3E-03
7	High	Yes	No	9.3E-03
8	High	Yes	Yes	9.3E-04

Table B-10 E-1: Delay Implementation

Crew Failure Scenario	Performance-Influencing Factors			Mean HEP
	Reluctance & Viable Alternative	Assessment of Margin	Additional Cues	
1	Exists	Incorrect	No	1.7E-01
2	Exists	Incorrect	Yes	1.1E-02
3	Exists	Correct	No	3.8E-02
4	Exists	Correct	Yes	6.5E-03
5	Absent	Incorrect	No	3.4E-03
6	Absent	Incorrect	Yes	2.2E-04
7	Absent	Correct		1.7E-05

Table B-11 E-2: Critical Data Not Checked with Appropriate Frequency

Crew Failure Scenario	Performance-Influencing Factors				Mean HEP
	Monitoring Optimized	Importance of Data Understood	Match with Expectations	Alarm	
1	No	No	Poor	No	4.3E-01
2	No	No	Poor	Yes	1.0E-02
3	No	No	Good	No	3.2E-02
4	No	No	Good	Yes	8.5E-03
5	No	Yes	Poor	No	1.4E-02
6	No	Yes	Poor	Yes	3.2E-04
7	No	Yes	Good	No	1.3E-02
8	No	Yes	Good	Yes	2.3E-03
9	Yes		Poor	No	1.3E-02
10	Yes		Poor	Yes	2.5E-04
11	Yes		Good	No	2.3E-03
12	Yes		Good	Yes	4.9E-05

Table B-12 E-3: Failure to Initiate Execution

Crew Failure Scenario	Performance-Influencing Factors			Mean HEP
	Immediacy	Workload	Recovery Potential	
1	No	High	No	1.5E-01
2	No	High	Yes	1.6E-02
3	No	Low	No	8.2E-03
4	No	Low	Yes	8.2E-04
5	Yes			1.4E-04

Table B-13 E-4: Failure to Correctly Execute Response (Simple Task)

Crew Failure Scenario	Performance-Influencing Factors			Mean HEP
	HSI	Workload	Recovery Potential	
1	Poor	High	No	3.3E-02
2	Poor	High	Yes	6.6E-03
3	Poor	Low	No	3.3E-02
4	Poor	Low	Yes	6.6E-03
5	Nominal	High	No	9.3E-06
6	Nominal	High	Yes	1.6E-06
7	Nominal	Low	No	9.3E-06
8	Nominal	Low	Yes	1.6E-06

Table B-14 E-5: Failure to Correctly Execute Response (Complex Task)

Crew Failure Scenario	Performance-Influencing Factors				Mean HEP
	Execution Straightforward	Training	Work Practice	Recovery Potential	
1	No	Poor	Poor	No	E-1
2	No	Poor	Poor	Yes	1.6E-02
3	No	Poor	Good	No	5.1E-02
4	No	Poor	Good	Yes	5.1E-03
5	No	Good	Poor	No	9.6E-03
6	No	Good	Poor	Yes	9.6E-04
7	No	Good	Good	No	3.8E-03
8	No	Good	Good	Yes	3.8E-04
9	Yes	Poor	Poor	No	9.6E-03
10	Yes	Poor	Poor	Yes	1.3E-04
11	Yes	Poor	Good	No	9.8E-04
12	Yes	Poor	Good	Yes	5.7E-05
13	Yes	Good	Poor	No	8.0E-04
14	Yes	Good	Poor	Yes	8.0E-05
15	Yes	Good	Good	No	8.0E-05
16	Yes	Good	Good	Yes	1.0E-05

APPENDIX C
SAMPLE ANALYSES USING IDHEAS AT-POWER

This appendix presents sample analyses for each of the human failure events that the study used to test the IDHEAS AT-POWER method. The samples were taken from the analyses performed by the project team (Team 5). Note that in the original analyses Crew Failure Mode AP-2 (Misread or Skip Step in Procedure) was identified as applicable for critical tasks that solely consisted of execution activities. These analyses have been corrected to remove Crew Failure Mode AP-2 because the crew failure mode is not applicable to execution tasks. An outline of the three scenarios and associated human failure events is provided below.

Scenario 1: Uncomplicated Steam Generator Tube Rupture

- **HFE 1:** Failure to isolate the ruptured steam generator and control pressure below the SG PORV setpoint before SG PORV opening.

Scenario 2: Loss of Feedwater with Misleading AFW Flow Indicator

- **HFE 2:** Failure to establish B&F within 45 minutes of the reactor trip, given that the crews initiate a manual reactor trip before an automatic reactor trip.

Scenario 3: Electrical Fire resulting in Loss of RCP Seal Cooling and Delayed Seal Injection

- **HFE 3:** Failure to restore CCW to the RCP thermal barrier heat exchangers by re-opening FCV-626.
- **HFE 4:** Failure to trip the RCPs during a loss of all seal cooling and injection.
- **HFE 5:** Failure to depressurize the RCS during a small loss of coolant accident (SLOCA).

C.1 Human Failure Event 1

C.1.1 PRA Scenario Description, Expected Operator Response and HFE Definition

The plant is a 4-loop Westinghouse pressurized water reactor (PWR). While operating at power, a tube rupture occurs in steam generator (SG) C. The leak size is about 500 GPM at 100% power. All participating crew members are in the control room (Shift Manager, Unit Supervisor, Shift Technical Advisor and two Reactor Operators).

The SGTR is sufficient to cause nearly immediate (less than 1 minute) alarms of secondary radiation (e.g., main steam line N16 and blowdown, condenser radiation alarms) and other abnormal indications/alarms such as lowering pressurizer pressure. The crew will either manually trip the reactor or there will be an automatic reactor trip and subsequent safety injection.

HFE 1 is defined as failure to isolate the ruptured steam generator and control pressure below the SG PORV setpoint before SG PORV opening.

Required operator actions include:

- Isolate the ruptured SG (feedwater and main steam isolation valves closed).

- Maintain RCS pressure below the SG PORV setpoint by cooling down the RCS (cooling the secondary by dumping steam and depressurizing the RCS).

To achieve success, the operators must isolate the ruptured steam generator and control pressure below the SG PORV setpoint before the SG PORVs open. The consequence of failure is a radiological release to the environment.

C.1.2 Crew Response Diagram (CRD) and Task Analysis

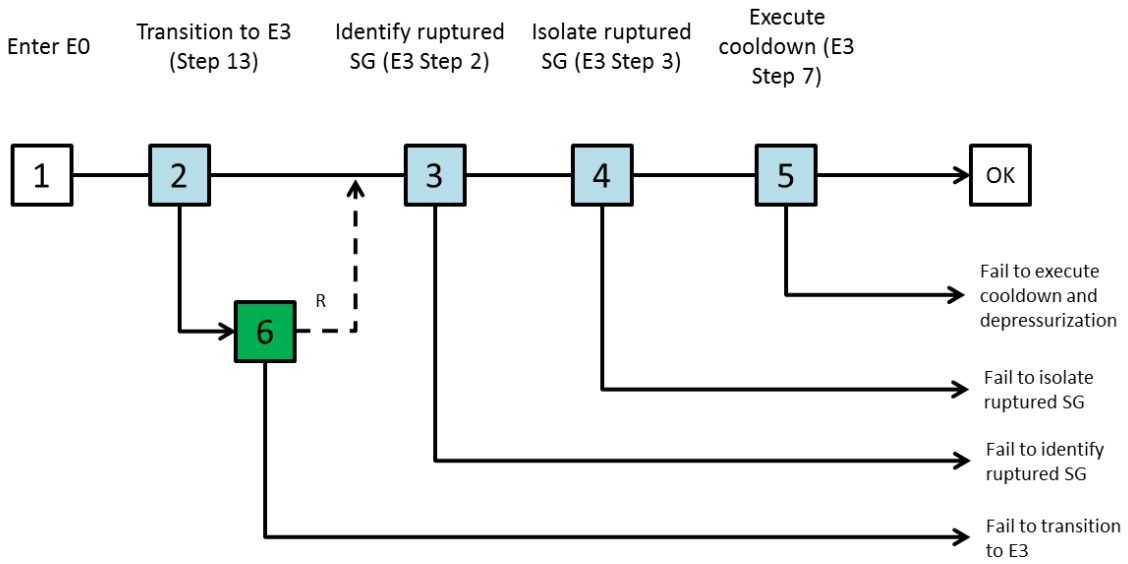


Figure C-1 Crew Response Diagram for HFE 1

C.1.2.1 Node 1: Enter E-0

When the reactor trips, the operators will immediately enter E-0. We assume they need SI, so there is no transfer to ES-01. There are no critical tasks associated with this node. This is a highly trained action, and we assume success at this step.

C.1.2.2 Node 2: Transfer to E-3 at step 13 of E-0

Step 13 of E-0 provides direction to transition to E-3 if key cues occur at this step. The leak size is about 500 GPM at 100% power. The SGTR is sufficient to cause nearly immediate (less than 1 minute) alarms of secondary radiation and other abnormal indications/alarms such as lowering pressurizer pressure. It takes about 8-12 minutes to get to Step 13, thus the crew is very likely to receive the alarms when they get to the step and identify there is an SGTR.

The critical task associated with this node is to check indications to identify if SG tubes are intact or ruptured. All four indications associated with this step are expected to be abnormal, therefore they are expected to reinforce each other, and the crew is highly likely to make a correct diagnosis and proceed to E-3.

Procedural Step (E-0 Step 13):
CHECK If SG Tubes Are Intact:

- Main steamline radiation - NORMAL
- IF SG blowdown in service, THEN SG blowdown radiation - NORMAL
- CARS pump radiation - NORMAL
- NO SG level rising in an uncontrolled manner

RNO: GO TO 0POP05-EO-EO30, STEAM GENERATOR TUBE RUPTURE, Step 1.

- MONITOR Critical Safety Functions.
- WHEN Addendum 5 of this procedure is complete, THEN NORMAL Restoration Procedures may be IMPLEMENTED.

C.1.2.3 Node 3: Identify ruptured SG at step 2 of E-3

When the crew enters E3, they are likely aware of the SGTR. Step 2 of E-3 will direct them to identify which SG is ruptured. The critical task associated with this node is to check indications on the SGs and identify which SG is ruptured. Any of the indications in this step can be used to identify the ruptured SG.

Procedural Step (E-3, Step 2):

IDENTIFY Ruptured SG(s):	**PERFORM the following:**
o Unexpected rise in any SG NR level OR o High radiation from any SG sample. OR o High radiation from any SG steamline OR o High radiation from any SG blowdown line	a. WHEN ruptured SG(s) identified, THEN PERFORM Steps 3 through 7, OBSERVE CAUTIONS and NOTES prior to Step 3, Step 4, Step 5, and Step 7 b. GO TO Step 8.

C.1.2.4 Node 4: Isolate Ruptured SG at Step 3

Once the crew has identified the ruptured SG, they are directed by procedure to isolate the SG. This includes multiple steps and is therefore a complex execution task.

Procedural Step (E-3, Step 3):
ISOLATE Flow From Ruptured SG(s):

___ a. ADJUST ruptured SG(s) PORV controller setpoint to BETWEEN 1260 PSIG AND 1265 PSIG (QDPS PRI/SEC)
___ b. CHECK ruptured SG(s) PORV controller - IN AUTO controller in AUTO.
___ c. CHECK ruptured SG(s) PORV - CLOSED
___ d. VERIFY blowdown isolation valve(s) from ruptured SG(s) - CLOSED
___ e. CHECK SG 1D(2D) - RUPTURED
___ f. VERIFY at least one motor-driven AFW pump – RUNNING
___ g. ISOLATE steam supply to turbine-driven AFW pump
    ___ 1) RESET SI
    ___ 2) RESET SG LO-LO level AFW actuations
    ___ 3) TRIP turbine-driven AFW pump
    ___ 4) CLOSE turbine-driven AFW pump
    ___ 5) DISPATCH operator to OPEN breaker E1D11(E2D11)/5C:
    ___ 6) ENSURE turbine-driven AFW pump trip/throttle valve closed
___ h. CLOSE ruptured SG(s) MSIV(s) and MSIB(s)

C.1.2.5 Node 5: Perform a cooldown at Step 7

After the ruptured SG is isolated, the crew will need to cooldown and depressurize the RCS to control pressure below SG PORV set point. This is a complex execution task.

Procedural Step (E-3, Step 7):
INITIATE RCS Cooldown:
___ a. DETERMINE required core exit temperature based on ruptured SG pressure (QDPS MAX QUAD T/C AVG):
___ b. CHECK pressurizer pressure LESS THAN 1985 PSIG
___ c. BLOCK Low Steamline Pressure SI
___ d. CHECK condenser – AVAILABLE
___ e. CHECK steam dump in
___ f. CHECK RCS TAVG - LESS THAN
___ g. PLACE steam dump "INTLK SEL" switches to BYPASS INTERLCK.
___ h. DUMP steam to condenser from intact SG(s) at maximum rate
___ i. Core exit T/Cs - LESS
___ j. STOP RCS cooldown
___ k. MAINTAIN core exit TCs – LESS THAN REQUIRED TEMPERATURE

C.1.2.6 Node 6: E-0 Step 22 (Recovery)

Step 22 is a potential recovery step to transition from E-0 to E-3, if they fail to transition at step 13. E-0, Step 22 allows the crew to enter E-3 if the level in any SG continued to rise in an uncontrolling manner.

Procedural Step (E-0, Step 22b):

___ b. CONTROL AFW flow to maintain NR levels BETWEEN 22% and 50%	**RNO:** b. IF NR level in any SG continues to rise in an uncontrolled manner, THEN GO TO 0POP05-EO-EO30, STEAM GENERATOR TUBE RUPTURE, Step 1. AND MONITOR Critical Safety Functions

C.1.2.7 Task Analysis

Table C-1 Task Analysis Table for HFE 1

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information
2	1	Identify SGTR	Data collection Interpretation Procedure transfer	There are multiple available indicators that can be used to identify the SGTR.
3	2	Identify which SG is ruptured	Data collection Interpretation	Any one of four indications in the procedure would cue the crew to identify the ruptured SG.
4	3	Isolate ruptured SG	Execution	This is a complex execution step.

5	4	Cooldown and control pressure	Execution	This is a complex execution step.

C.1.3 Timeline

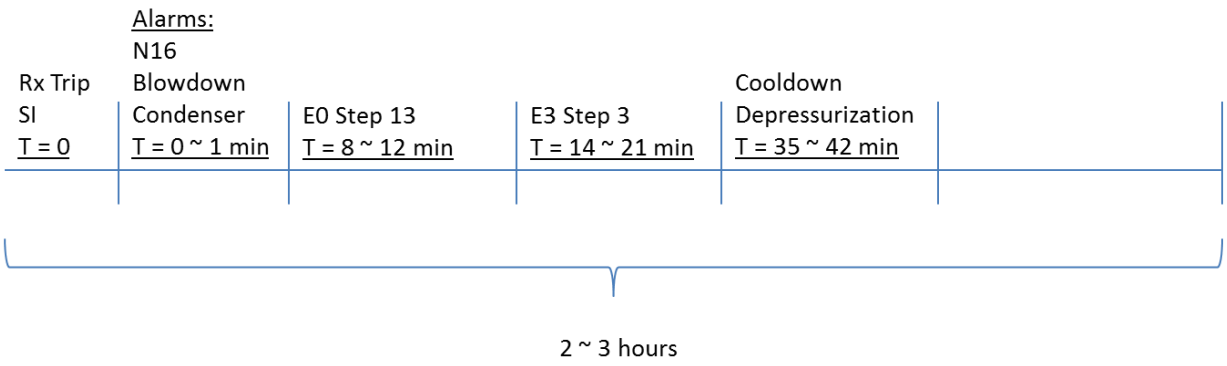


Figure C-2 Timeline for HFE 1

Within the first few minutes of the scenario the crew will either manually trip the reactor or there will be automatic reactor trip, likely due to low pressurizer pressure. It is assumed that the crew manually trips the reactor, and the reactor trip signifies time 0 in the above timeline.

Indications of the SGTR will be present within the first 1-2 minutes of the event. In particular, alarms of secondary radiation (main steam line N16 and blowdown, condenser radiation alarms).

Following the reactor trip, the crew will enter procedure E-0. It is expected that the crew will take approximately 8-12 minutes to proceed through E-0 to step 13, at which time the crew will diagnose the SGTR and transition to procedure E-3.

The crew will then proceed through procedure E-3 to identify and isolate the ruptured SG. There are multiple execution steps in this procedure, and it will likely take the crew 6-9 minutes to execute these actions.

Finally, the crew will begin to cooldown the RCS and control pressure below the PORV setpoint. This is a complex control action and will take approximately 21 minutes to execute before the plant is stable.

It is expected that the crew will take no more than 42 minutes to achieve successful cooldown and depressurization. Based on thermodynamic calculations, the time window to perform the required actions for this event is approximately 3 hours.

The actions required to achieve success are determined to be feasible because there is adequate time available for the operators to make their way through the appropriate procedures and execute cooldown and depressurization actions before the PORV setpoint is reached.

C.1.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees

C.1.4.1 HFE 1, Critical Task 1

Table C-2 CFM Selection Table for HFE 1, Critical Task 1

CRD Node	2 – Transfer from E-0 to E-3	
Critical Task	1 – Identify SGTR	
CFMs	**Applicable? (Yes/No)**	**Justification**
AP-1: Key Alarm not Attended to	No	Not applicable because cued off procedure.
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	Written procedure in use.
SA-1: Data Misleading or Not Available	No	Four diverse cues must be missed to fail.
SA-2: Wrong Data Source Attended To	No	Four diverse cues must be missed to fail.
SA-3: Critical Data Incorrectly Processed/Misperceived	No	Four diverse cues must be missed to fail.
SA-4: Critical Data Dismissed/Discounted	Yes	Yes, but there is no credible alternative data.
SA-5: Premature Termination of Critical Data Collection	No	Not a monitoring task. Check only.
RP-1: Misinterpret Procedures	Yes	Yes, but the procedure is simple and unlikely to be misinterpreted.
RP-2: Choose Inappropriate Strategy	No	Straightforward decision.
E-1: Delay Implementation	No	Not an execution task.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	Not an execution task.
E-3: Fail to Initiate Execution	No	Not an execution task.
E-4: Fail to Correctly Execute Response (Simple Task)	No	Not an execution task.
E-5: Fail to Correctly Execute Response (Complex Task)	No	Not an execution task.

Table C-3 Evaluation of CFM AP-2 for HFE 1, Critical Task 1

AP-2: Misread or Skip Critical Step(s) in Procedure		
PSF	**Assessment**	**Justification**
Workload	*Low*	Workload is not greater than crew can manage.
Procedure	*Simple*	Procedure is trained on frequently and straightforward.

Compensatory Factors	*N/A*	N/A
Recovery Potential	*Yes*	Recovery is possible at Step 22 of E-0.
Crew Failure Scenario #		*14*

Table C-4 Evaluation of CFM SA-4 for HFE 1, Critical Task 1

SA-4: Critical Data Dismissed/Discounted		
PSF	**Assessment**	**Justification**
Valid Alternative/ Deviation Scenario	*No*	No alternative available.
Inappropriate Bias	*N/A*	*N/A*
Indications Reliable	*N/A*	*N/A*
Confirmatory Information	*N/A*	*N/A*
Recovery Potential	*N/A*	*N/A*
Crew Failure Scenario #		*8*

Table C-5 Evaluation of CFM RP-1 for HFE 1, Critical Task 1

RP-1: Misinterpret Procedures		
PSF	**Assessment**	**Justification**
Procedures Open to Misinterpretation	*No*	Procedure is straightforward and often used.
Workload	*N/A*	*N/A*
Training/Experience	*N/A*	*N/A*
Recovery Potential	*N/A*	*N/A*
Crew Failure Scenario #		*8*

C.1.4.2 HFE 1, Critical Task 2

Table C-6 CFM Selection Table for HFE 1, Critical Task 2

CRD Node #	3 – E-3, Step 2	
Critical Task #	2 – Check indications to identify ruptured SG	
CFMs	**Applicable? (Yes/No)**	**Justification**
AP-1: Key Alarm not Attended to	No	Cued off procedure.
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	A written procedure is in use.
SA-1: Data Misleading or Not Available	No	Four diverse cues must be missed to fail.
SA-2: Wrong Data Source Attended To	No	Four diverse cues must be missed to fail.

SA-3: Critical Data Incorrectly Processed/Misperceived	No	Four diverse cues must be missed to fail.
SA-4: Critical Data Dismissed/Discounted	Yes	This is possible, but there is no credible alternative.
SA-5: Premature Termination of Critical Data Collection	No	This is not a monitoring action.
RP-1: Misinterpret Procedures	Yes	Applicable, but the procedure is simple and not likely to be misinterpreted.
RP-2: Choose Inappropriate Strategy	No	No choice of strategy.
E-1: Delay Implementation	No	Not an execution task.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	Not an execution task.
E-3: Fail to Initiate Execution	No	Not an execution task.
E-4: Fail to Correctly Execute Response (Simple Task)	No	Not an execution task.
E-5: Fail to Correctly Execute Response (Complex Task)	No	Not an execution task.

Table C-7 Evaluation of CFM AP-2 for HFE 1, Critical Task 2

AP-2: Misread or Skip Critical Step(s) in Procedure		
PSF	**Assessment**	**Justification**
Workload	*Low*	Workload is not greater than crew can manage.
Procedure	*Simple*	Procedure is trained on frequently and straightforward.
Compensatory Factors	*N/A*	N/A
Recovery Potential	*Yes*	Recovery is possible from multiple cues. Also, Step 3 directs the crew to isolate the ruptured SG. This requires the crew to have identified the ruptured SG, so if Step 2 had been misread or skipped this is an additional cue to revisit the identification.
Crew Failure Scenario #		*14*

Table C-8 Evaluation of CFM SA-4 for HFE 1, Critical Task 2

SA-4: Critical Data Dismissed/Discounted		
PSF	**Assessment**	**Justification**
Valid Alternative/ Deviation Scenario	*No*	No credible alternative.
Inappropriate Bias	*N/A*	*N/A*
Indications Reliable	*N/A*	*N/A*

Confirmatory Information	*N/A*	*N/A*
Recovery Potential	*N/A*	*N/A*
Crew Failure Scenario #		*16*

Table C-9 Evaluation of CFM RP-1 for HFE 1, Critical Task 2

RP-1: Misinterpret Procedures		
PSF	**Assessment**	**Justification**
Procedures Open to Misinterpretation	*No*	Procedure is straightforward and often used.
Workload	*N/A*	*N/A*
Training/Experience	*N/A*	*N/A*
Recovery Potential	*N/A*	*N/A*
Crew Failure Scenario #		*8*

C.1.4.3 HFE 1, Critical Task 3

Table C-10 CFM Selection Table for HFE 1, Critical Task 3

CRD Node #	4 – E-3, Step 4	
Critical Task #	3 – Isolate ruptured SG	
CFMs	**Applicable? (Yes/No)**	**Justification**
AP-1: Key Alarm not Attended to	No	No alarm response required.
AP-2: Misread or Skip Critical Step(s) in Procedure*	No	This is only an execution task.
SA-1: Data Misleading or Not Available	No	This is only an execution task.
SA-2: Wrong Data Source Attended To	No	This is only an execution task.
SA-3: Critical Data Incorrectly Processed/Misperceived	No	This is only an execution task.
SA-4: Critical Data Dismissed/Discounted	No	This is only an execution task.
SA-5: Premature Termination of Critical Data Collection	No	This is only an execution task.
RP-1: Misinterpret Procedures	No	This is only an execution task.
RP-2: Choose Inappropriate Strategy	No	This is only an execution task.
E-1: Delay Implementation	Yes	Decision to execute has already been made at this point.

E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	Data monitoring not required.
E-3: Fail to Initiate Execution	Yes	Possible, but unlikely, as it is the only action required at this time in the event.
E-4: Fail to Correctly Execute Response (Simple Task)	No	This is a complex task.
E-5: Fail to Correctly Execute Response (Complex Task)	Yes	This is a complex execution with multiple procedural steps.

* CFM AP-2 was identified as applicable for Critical Task 3 in the original analysis.

Table C-11 Evaluation of CFM E-1 for HFE 1, Critical Task 3

E-1: Delay Implementation		
PSF	**Assessment**	**Justification**
Reluctance and Viable Alternative	*Absent*	No viable alternative.
Assessment of Margin	*Correct*	
Additional Cues	*N/A*	N/A
Crew Failure Scenario #		*7*

Table C-12 Evaluation of CFM E-3 for HFE 1, Critical Task 3

E-3: Fail to Initiate Execution		
PSF	**Assessment**	**Justification**
Immediacy	*Yes*	Only action in operator mental cue.
Workload	*N/A*	N/A
Recovery Potential	*N/A*	N/A
Crew Failure Scenario #		*5*

Table C-13 Evaluation of CFM E-5 for HFE 1, Critical Task 3

E-5: Fail to Correctly Execute Response (Complex Task)		
PSF	**Assessment**	**Justification**
Execution Straightforward	*Yes*	Directed by procedures.
Training	*Good*	Well-trained action.
Work Practices	*Good*	Use of human performance tools.
Recovery Potential	*No*	No recovery.
Crew Failure Scenario #		*13*

C.1.4.4 HFE 1, Critical Task 4

Table C-14 CFM Selection Table for HFE 1, Critical Task 4

CRD Node #	5 – E-3, Step 7	
Critical Task #	4 – Cooldown and Control Pressure	
CFMs	**Applicable? (Yes/No)**	**Justification**
AP-1: Key Alarm not Attended to	No	No alarm response required.
AP-2: Misread or Skip Critical Step(s) in Procedure*	No	This is only an execution task.
SA-1: Data Misleading or Not Available	No	This is only an execution task.
SA-2: Wrong Data Source Attended To	No	This is only an execution task.
SA-3: Critical Data Incorrectly Processed/Misperceived	No	This is only an execution task.
SA-4: Critical Data Dismissed/Discounted	No	This is only an execution task.
SA-5: Premature Termination of Critical Data Collection	No	This is only an execution task.
RP-1: Misinterpret Procedures	No	This is only an execution task.
RP-2: Choose Inappropriate Strategy	No	This is only an execution task.
E-1: Delay Implementation	Yes	The decision to execute has already been made.
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	Data monitoring not required as part of this task.
E-3: Fail to Initiate Execution	Yes	Possible, but unlikely, given that this is the only action required of the cue and is highly trained.
E-4: Fail to Correctly Execute Response (Simple Task)	No	This is a complex task.
E-5: Fail to Correctly Execute Response (Complex Task)	Yes	This is a complex execution with multiple steps.

*CFM AP-2 was identified as applicable for Critical Task 4 in the original analysis.

Table C-15 Evaluation of CFM E-3 for HFE 1, Critical Task 4

E-3: Fail to Initiate Execution		
PSF	**Assessment**	**Justification**
Immediacy	*Yes*	Only action in operator mental cue.
Workload	*N/A*	N/A
Recovery Potential	*N/A*	N/A
Crew Failure Scenario #		*5*

Table C-16 Evaluation of CFM E-5 for HFE 1, Critical Task 4

E-5: Fail to Correctly Execute Response (Complex Task)		
PSF	**Assessment**	**Justification**
Execution Straightforward	*No*	Complex control action.
Training	*Good*	Well-trained scenario.
Work Practices	*Good*	Use of human performance tools expected.
Recovery Potential	*No*	No recovery.
Crew Failure Scenario #		*7*

C.1.5 Summary of Analysis

This is a standard SGTR scenario. The crew is expected to handle this scenario without difficulties for the following reasons:

- The crew is highly trained for this scenario
- Indications are clear, and there are multiple diverse indications
- Workload is not expected to be higher than the crew can manage
- The time window to perform the required actions is estimated to be 3 hours, which is longer than the required time (42 minutes)
- Environmental factors are nominal

The appropriate crew response to an SGTR event is to eventually enter the Steam Generator Tube Rupture Procedure E-3. Immediately after reactor trip, the crew is expected to enter the Reactor Trip procedure E-0 and must work through E-0 and subsequent procedures to reach an opportunity to transfer to E-3. Step 13 of E-0 is the first opportunity transfer to E-3, and it is very likely because the crew is expected to get cues when they get to this step. If they miss this opportunity, there multiple opportunities to recover.

If/when the crew enters E-3, the scenario proceeds in response to the crew's actions with no failures or other complicating factors induced. That is, the plant response will be based on what the crew does in carrying out procedure E-3. Step 2 of E-3 will direct the crew to identify which SG is ruptured. Steps 3 and 4 will ask the crew to isolate the rupture SG. Steps 7 through 19 provides guidance to cooldown and depressurize the RCS to control the pressure under the SG set point. SG isolation, RCS cooldown and RCS depressurization are complex execution tasks.

Table C-17 HEP Calculation Table for HFE 1

CRD Node #	Critical Task #	CFM	Crew Failure Scenario #	HEP
2	1	AP-2: Misread or Skip Critical Step(s) in Procedure	14	1.2E-04

2	1	SA-4: Critical Data Dismissed/Discounted	16	0
2	1	RP-1: Misinterpret Procedures	8	0
3	2	AP-2: Misread or Skip Critical Step(s) in Procedure	14	1.2E-04
3	2	SA-4: Critical Data Dismissed/Discounted	16	0
3	2	RP-1: Misinterpret Procedures	8	0
4	3	E-1: Delay Implementation	7	1.7E-05
4	3	E-3: Fail to Initiate Execution	5	1.4E-04
4	3	E-5: Fail to Correctly Execute Response (Complex Task)	13	8.0E-04
5	4	E-1: Delay Implementation	7	1.7E-05
5	4	E-3: Fail to Initiate Execution	5	1.4E-04
5	4	E-5: Fail to Correctly Execute Response (Complex Task)	7	3.8E-03
			Total HEP:	**4.4E-3**

* CFM AP-2 was identified as applicable for Critical Tasks 3 and 4 in the original analysis. The total HEP is adjusted for deleting the CFM from the applicable CFMs for the two critical tasks.

C.2 Human Failure Event 2

C.2.1 PRA Scenario Description, Expected Operator Response and HFE Definition

Plant technical information:

- 4-loop Westinghouse pressurized water reactor (PWR)
- There are three main feedwater (MFW) pumps: 11, 12 and 13
- There are four auxiliary feedwater (AFW) pumps: 11, 12, 13 and 14. AFW pump 14 is turbine-driven and the other three motor-driven.

Situation from start:

- The Shift Technical Advisor (STA) 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 (Shift Manager, Unit Supervisor, 2 Reactor Operators)
- The plant is operating at 100%
- Core burnup is 19,000 MWD/MTU (End of life)

Total loss of feedwater:

During routine operation at power, MFW pump 11 is lost, and MFW pumps 12 and 13 trip within the next 10 seconds. The startup feedpump, which receives an auto start signal after the turbine driven feed pump, cannot be started. If the crew doesn't trip the reactor manually the reactor will trip on low SG level (20%).

At autostart, AFW pump 14 overspeeds and causes damage that cannot be repaired. AFW pump 11 has a seized shaft and trips and is therefore not available. AFW pump 13 starts but the shaft shears and no flow is indicated.

AFW pump 12 starts automatically and indicates full flow, but this flow will not reach (feed) the steam generators (SGs) because a manual recirculation valve is mis-positioned (it is open). There is no indication of the valve's position in the control room. Since there is no AFW flow to the SGs, the SG levels will go down rapidly before the reactor is tripped.

In reality, criteria to start FRH1 are met. But because of the indicated flow from AFW pump 12, the plant computer will not show a red path on the heatsink status tree.

Figure C-3~~Figure C-3~~ is the event tree with the sequence highlighted.

Expected operator response:

The appropriate crew response to loss of heatsink is to enter the Response to Loss of Secondary Heat Sink procedure (FRH1) to start bleed and feed (B&F; primary B&F, with feed from safety injection and bleed through the pressurizer PORVs).

All attempts to establish AFW before the B&F initiation will fail.

Assuming the crew manually trips the reactor within approximately 30 - 45 seconds of the loss of feedwater, they will have approximately 45 minutes to initiate B&F before core damage (CD).

HFE definition:

Failure to establish B&F within 45 minutes of the reactor trip, given that the crews initiate a manual reactor trip before an automatic reactor trip.

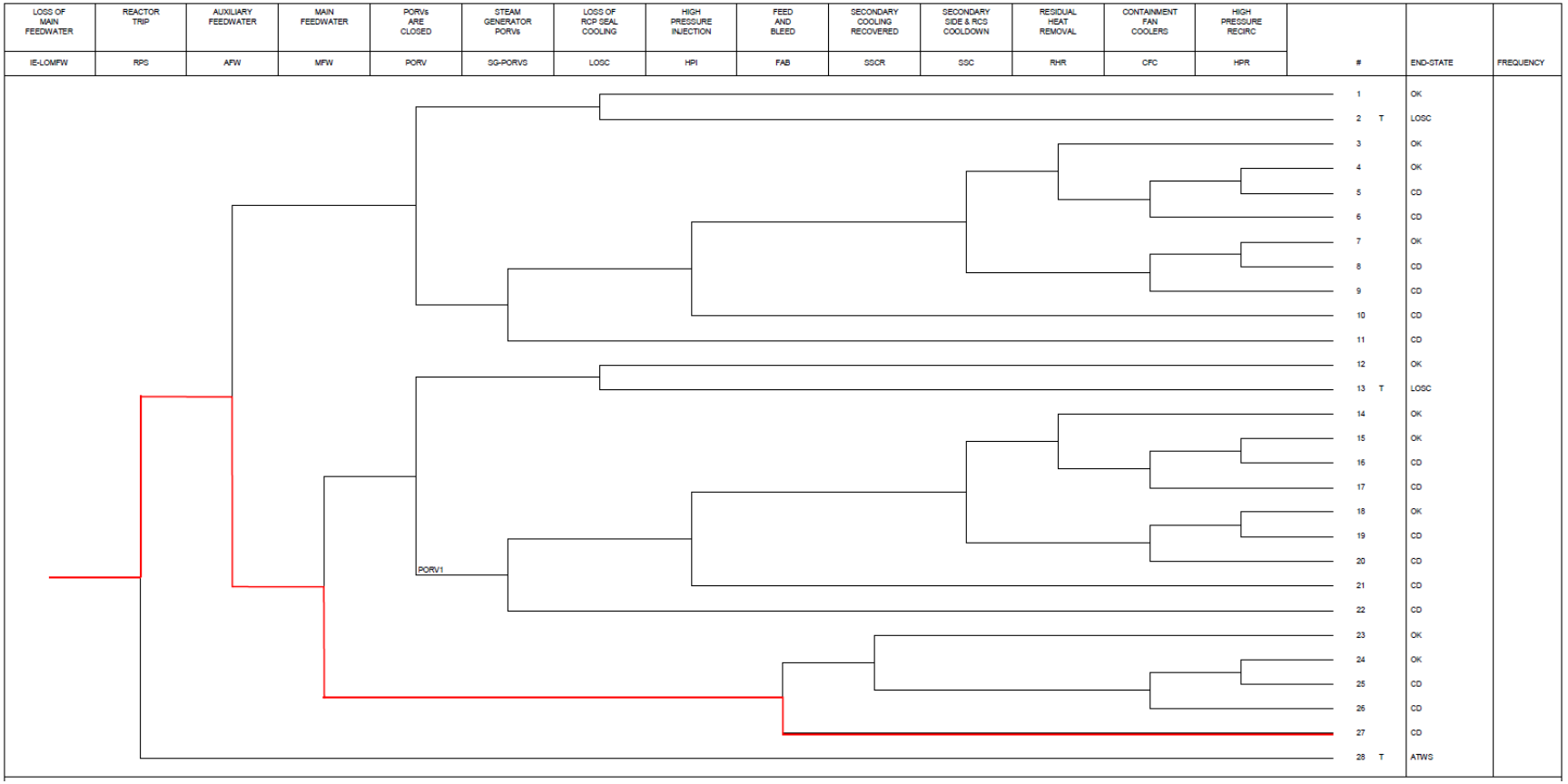


Figure C-3 Loss of Main Feedwater Event Tree for HFE 2

C.2.2 Crew Response Diagram (CRD) and Task Analysis

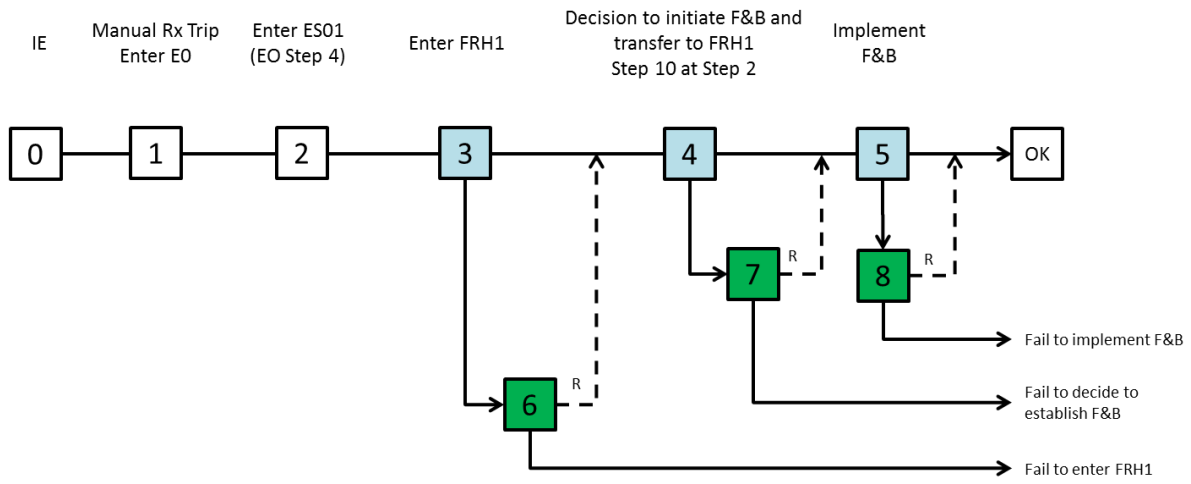


Figure C-4 Crew Response Diagram for HFE 2

C.2.2.1 Node 0: IE

Node 0 in Figure C-4~~Figure C-4~~ represents the initiating event – total LOFW. There are no critical tasks associated with it.

C.2.2.2 Node 1: Manual reactor trip and enter E0

Many cues will occur after the total LOFW, including FW alarms (MFW trip and alarms), the rapidly decreasing SG levels, SG Low-Level Alarms, and SG Low-Low Level Alarms. The crew is well trained on LOFW. It is assumed that the crew manually trips the reactor within approximately 30 - 45 seconds of total LOFW. The timing of a reactor trip determines how low and how fast the SG levels drop and the time available before F&B must be initiated.

Immediately after the reactor trip, the crew will enter the Reactor Trip or Safety Injection procedure (E0). Success of entry of E0 is assumed given training.

This node is an HFE boundary condition event as defined in the scenario description. There are no critical tasks associated with it.

C.2.2.3 Node 2: Enter ES01 from E0 Step 4

The first four steps of E0 verify reactor trip, turbine trip, power to the AC ESF busses, and the status of SI. They are considered memorized actions and will take approximately 4 minutes to complete. Since SI is neither actuated nor required in this case, the crew will transfer to ES01 from Step 4a RNO and start to monitor Critical Safety Functions.

Upon Step 5, the second operator will enter Addendum 5 while the first operator continues in EO00. At this point, Addendum 5 is the sole responsibility of the second operator and will take approximately 5 – 10 minutes. The crew would not wait for Addendum 5 to be completed to enter a subsequent procedure. The first steps are highly trained, thus entry of ES01 is assumed success. There are no critical tasks associated with it.

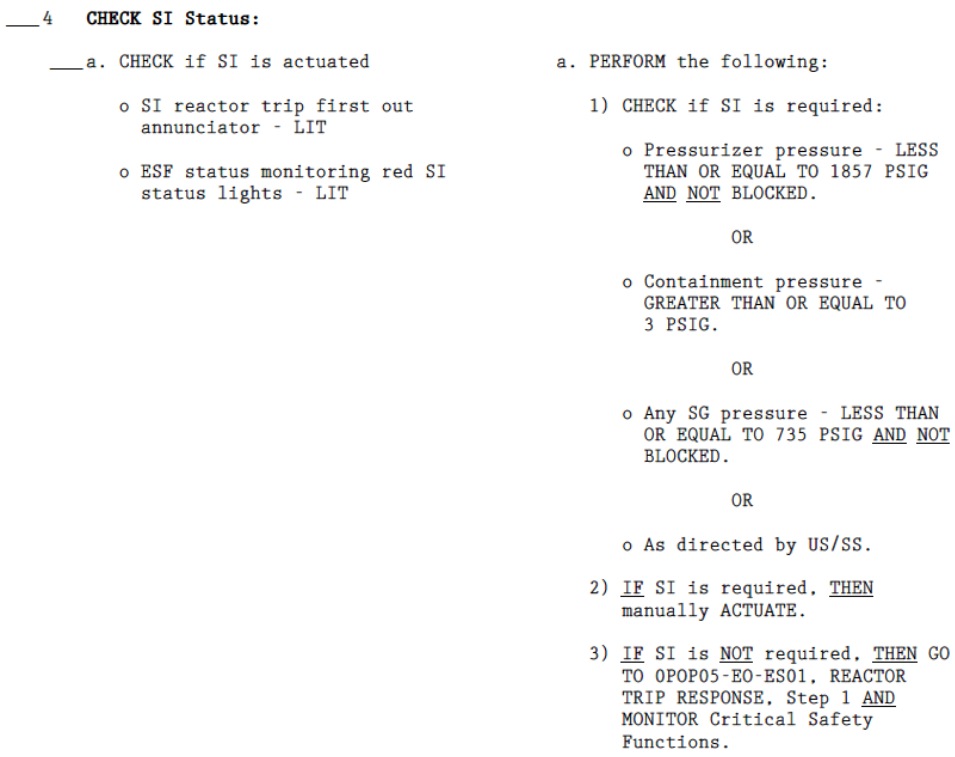


Figure C-5 Step 4a in Procedure E0

C.2.2.4 Node 3: Enter FRH1

The only path to initiate F&B is via FRH1 (Response to Loss of Secondary Heat Sink) in this scenario. In this plant the only direct path that will instruct entry into FRH1 is via the Critical Safety Function Status Tree (CSFST) for Heat Sink. The entry condition of FRH1 is a red path on the Heat Sink CSFST (0POP05-E0-F003), for which the crew is well trained. The crew will not start monitoring the critical safety functions until they are procedurally instructed to do so. In EO00, there are two opportunities for the crew to start monitoring the critical safety functions:

- Step 4a of EO00 where the crew transfers to Step 1 of ES01. This transfer is very likely because LOFW is unlikely to cause SI.
- Step 16 of EO00 after completion of Addendum 5.

The indications in the control room are easily accessible. However, symptom-based EOPs and the CSFSTs do not address the misaligned recirculation valve or allow for prompt diagnosis of loss of heat sink. This is because the crew is trained to rely on process computer (QDPS) displays to assess critical safety function status. As mentioned above, the QDPS will show a yellow rather than red path on the heat sink status tree due to the misleading AFW indication.

Several factors will help the crew realize FRH1 entry conditions have been met:

- First, the crew is trained on loss of main feedwater with mis-positioned AFW recirculation valves at least once every two years, and the plant had an operating experience of AFW recirculation valves being mis-positioned years ago. When they leave E0, the crew will

monitor feed flow and check AFW status by looking at multiple indications, including the SG tank levels. The SG levels will initially fall after the reactor trip. With a feed flow of 576 GPM, they are expected to come back on scale (NR) within five minutes. However, the level will continue to drop in this case. If the SG levels do not return and keep trending down with indicated AFW flow, the crew will realize that there is a problem with the AFW and then verify AFW flow with the AFW tank level on the plant computer, which will take about 30 seconds.

- Second, Step 3 of ES01 will instruct the crew to check feedwater flow. It takes 3 minutes to reach Step 3 after entry of ES01.
- Third, the STA is likely to be called at the beginning of this scenario and be active when the crew starts to monitor critical safety functions and reaches ES01 Step 3. One of the STA's responsibilities is to monitor the Critical Safety Functions (CSFs). Once the AFW flow problem is brought into attention, he or she will look at the AFW tank level to recognize that the criteria to start FRH1 are met.

When the crew realizes AFW is not reaching the SGs, they will try to establish AFW flow, for example, per guidance at ES01 Step 3 RNO. They will also send a plant operator to check the status of the recirculation valve. It will take approximately 10 - 20 minutes for the plant operator to report back to the crew on the status of the valve. However, any attempts to establish AFW before F&B will fail.

<u>The critical tasks associated with Node 3 include:</u>

- Monitoring the Heat Sink CSFST for Criterion 1 "NR Level in at least one SG greater than 14% [34%]"
- Monitoring the Heat Sink CSFST for Criterion 2 "Total AFW Flow to SGs greater than 576 GPM"

C.2.2.5 Node 4: Transfer to FRH1 Step 10

Step 1 verifies if secondary heat sink is required. Since the crew are already aware of loss of secondary heat sink when they enter FRH1, success at this step is assumed. Step 2 will guide the decision to establish F&B by checking SG WR level and pressurizer pressure. One of the F&B criteria is the SG WR level in at least two SGs is less than 50%. This criterion should be reached approximately 2 to 2.5 minutes after the LOFW. That is, this criterion should be met when the crew enters FRH1. Therefore, the crew will trip RCPs and transfer to Step 10 from Step 2 RNO.

2	**CHECK Secondary Heat Sink:** o SG wide range level in at least three intact SGs - GREATER THAN 50% [73%] o Pressurizer pressure - LESS THAN 2335 PSIG	PERFORM the following: a. TRIP all RCPs. b. GO TO Step 10, OBSERVE CAUTION prior to Step 10.

Figure C-6 Step 2 in Procedure FRH1

The critical tasks associated with Node 4 include:

- Evaluate SG WR level and pressurizer pressure and transfer to Step 10.

C.2.2.6 Node 5: Implement F&B

The crew is well trained (a minimum of once every two years) on F&B in the context of LOFW and with the input of SG WR levels. Although F&B has undesirable consequences and the crew will try to establish AFW flow (e.g., cross-connect AFW and close the recirculation valve) when they detect that there is no AFW flow, they will not hesitate to initiate F&B when the criteria are met. Nonetheless, there is expected to be some pressure or stress considering the potential cost associated with F&B.

F&B initiation includes starting high-head safety injection pumps (Steps 10) and opening pressurizer PORV (Step 12). It will take about 2 minutes to complete these actions. Note that the caution above Step 10 asks operators to implement F&B quickly.

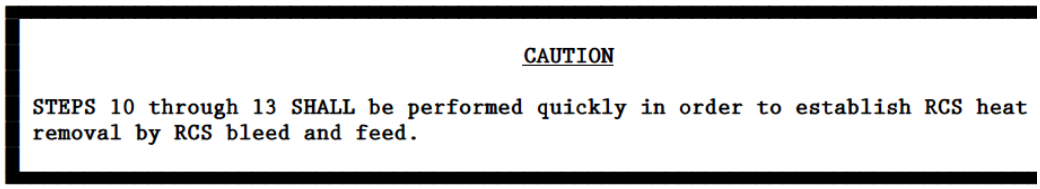


Figure C-7 Step 10 in Procedure FRH1

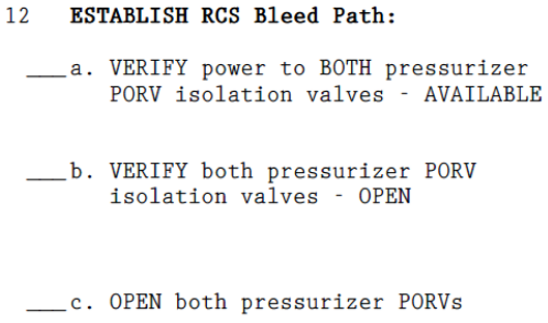


Figure C-8 Step 12 in Procedure FRH1

The critical tasks associated with Node 5 include:

- Step 10. Actuate SI
- Step 12. Establish RCS bleed path

C.2.2.7 Node 6: Recovery of Node 3

Criteria to enter FRH1 are not part of ES01. The Conditional Information Page for ES01 and the steps of ES-01 do not include any condition for transferring to FRH1. Thus, the decision to transfer to FRH1 is based on evaluation of the heat sink CSFST in parallel with the execution of ES01 steps.

Due to the misleading AFW flow indication, the CSFST will show a yellow path rather than a red path. In addition, ES01 Step 3 does not guarantee detection of the diverted AFW flow because the crew may simply check the AFW flow indication. Moreover, the instructions and goals of ES01 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.

If they fail to detect the AFW problem at Step 3 of ES01, Step 8 provides a recovery opportunity by instructing the operators to check and maintain the SG levels. When the operators cannot achieve the goal of the step, the AFW flow problem will be become apparent. It will take 5 minutes to reach Step 8 from Step 3. In addition, Step 18 also asks operators to maintain SG levels.

C.2.2.8 Node 7: Recovery of Node 4

If the F&B initiation criteria are not met when the crew reaches Step 2, the crew will not transfer to Step 10. In this case, Step 9 provides a recover opportunity to check the F&B initiation criteria. In addition, the first condition of Conditional Information Page (CIP) instructs the crew to continuously monitor SG WR levels and pressurizer pressure.

C.2.2.9 Node 8: Recovery of Node 5

Steps 11 and 13 of FRH1 instruct the operators to verify if B&F is properly initiated. This provides a recovery of failure to perform Steps 10 and 12. Relevant indications (e.g., HHSI pump status) are available in the control room.

C.2.2.10 Task analysis

Table C-18 Task Analysis for HFE 2

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information
3	1	Monitoring the Heat Sink CSFST for Criterion 1 “NR Level in at least one SG greater than 14% [34%]”	• Identify correct data source • Interpret plant parameter correctly (comparing against numerical criteria in procedure)	The criteria are numerical, requiring no additional judgment.
3	2	Monitoring the Heat Sink CSFST for Criterion 2 “Total AFW Flow to	• Identify correct data source • Interpret plant parameter correctly (comparing against	The criteria are numerical, requiring no additional judgment.

		SGs greater than 576 GPM"	numerical criteria in procedure)	
4	3	Evaluate SG WR level and pressurizer pressure and transfer to Step 10	• Identify correct data source • Interpret plant parameters correctly (comparing against numerical criteria in procedure and deciding to initiate F&B) • Transfer to Step 10	The criteria are numerical, requiring no additional judgment. In FR-H1 Step 2, the logic is not explicitly provided (the expected response is met if both criteria are met and not met if either criterion is not met, i.e., AND-logic for the expected response to be met).
5	4	Actuate SI and Establish RCS bleed path	Simple execution from the control room	Execution tasks are analyzed in an integral manner in IDHEAS.

C.2.3 Timeline

The timeline for HFE 2 is illustrated in Figure C-9~~Figure C-9~~. The green color represents actual events or boundary conditions, and the cyan color represents predicted events and estimates.

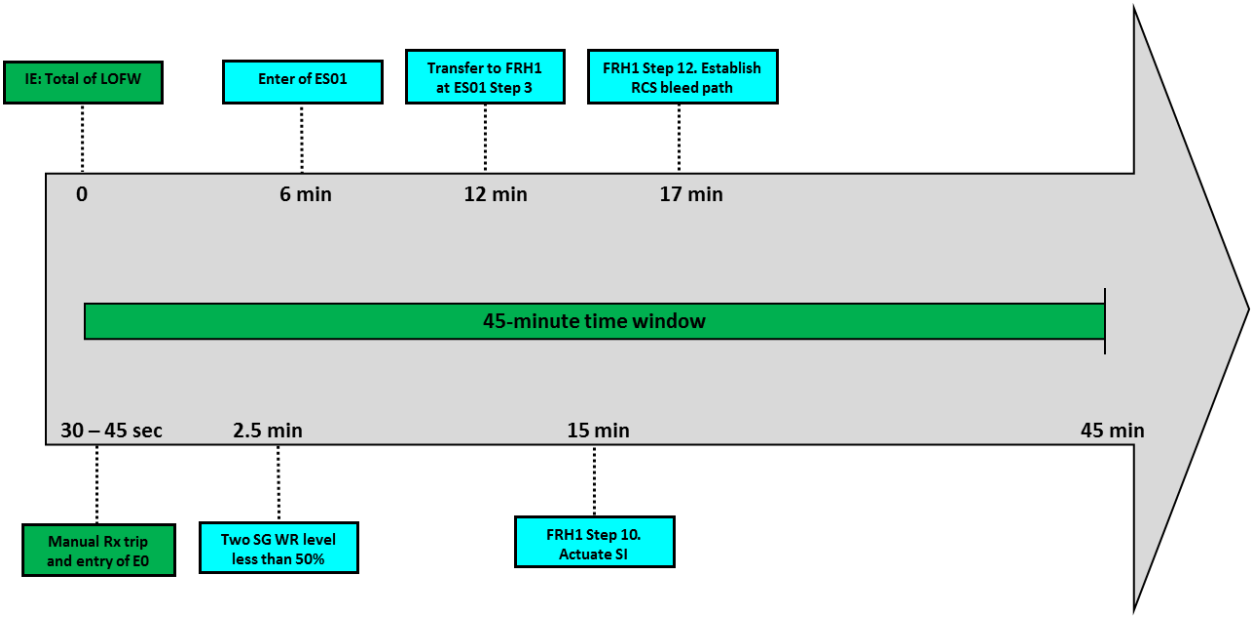


Figure C-9 Timeline for HFE 2

C.2.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees

C.2.4.1 Critical Task 1

Table C-19 CFM Selection Table for HFE 2, Critical Task 1

CRD Node	3		
Critical Task	1		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	Directed search by procedure.	
AP-2: Misread or Skip Critical Step(s) in Procedure	No	The CSFST is a single page with a simple logic presented in a flowchart format	
SA-1: Data Misleading or Not Available	No	Instrumentation works properly and indications are available in the MCR. The SG level indications are trending down since the start of the transient and reactor trip.	
SA-2: Wrong Data Source Attended To	Yes	Potentially applicable. WR levels could potentially be attended to instead of NR levels. They will indicate larger percentage values.	16
SA-3: Critical Data Misperceived	Yes	Potentially applicable. The level value expressed as a percentage may be misperceived.	16
SA-4: Critical Data Dismissed/Discounted	No	The level criterion is below what could be expected in a normal reactor trip situation.	
SA-5: Premature Termination of Critical Data Collection	No	The STA will periodically check the CSFST.	
RP-1: Misinterpret Procedures	No	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	No	No other strategy in procedure.	
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	Not an execution step	

Table C-20 Evaluation of CFM SA-2 for HFE 2, Critical Task 1

SA-2: Wrong Data Source Attended to		
PIF	**Assessment**	**Justification**
HSI	Good	NR and WR SG Level indications are collocated but labeled clearly
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.
Familiarity with Data Source	Good	NR and WR SG Levels
Recovery Potential	Yes	
Crew Failure Scenario #		16

Table C-21 Evaluation of CFM SA-3 for HFE 2, Critical Task 1

SA-3: Critical Data Misperceived		
PIF	**Assessment**	**Justification**
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	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.
Training	Good	Checking the CSFST is frequently performed and is one of the responsibilities of the STA.
Recovery Potential	Yes	
Crew Failure Scenario #		16

C.2.4.2 Critical Task 2

Table C-22 CFM Selection Table for HFE 2, Critical Task 2

CRD Node	3		
Critical Task	2		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	Directed search by procedure.	

AP-2: Misread or Skip Critical Step(s) in Procedure	No	The CSFST is a single page with a simple logic presented in a flowchart format	
SA-1: Data Misleading or Not Available	Yes	AFW is diverted by the mis-positioned recirculation valve.	9
SA-2: Wrong Data Source Attended To	No	There are several indications for assessing whether AFW is operating. They would collectively point to zero flow.	
SA-3: Critical Data Misperceived	No	Multiple indications would collectively point to zero flow.	
SA-4: Critical Data Dismissed/Discounted	No	Multiple indications would collectively point to zero flow.	
SA-5: Premature Termination of Critical Data Collection	No	The STA will periodically check the CSFST.	
RP-1: Misinterpret Procedures	No	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	No	No other strategy in procedure.	
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	Not an execution step	

Table C-23 Evaluation of CFM SA-1 for HFE 2, Critical Task 2

SA-1: Data Misleading or not Available		
PIF	**Assessment**	**Justification**
Alternate/Supplementary Source of Information	Yes	Multiple indications exist to verify the AFW flow.
Information Obviously Incorrect	No	Value is not pegged high or low.
Guidance to Seek Confirmatory Data	Yes	The crew is trained to monitor feed flow and check AFW status by looking at multiple indications, including the SG levels.
Distraction	Low	
Crew Failure Scenario #		5

C.2.4.3 Critical Task 3

Table C-24 CFM Selection Table for HFE 2, Critical Task 3

CRD Node	4		
Critical Task	3		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	Directed search by procedure.	
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable but unlikely.	14
SA-1: Data Misleading or Not Available	No	Instrumentation works properly and indications are available in the MCR.	
SA-2: Wrong Data Source Attended To	No	This 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 F&B criteria will be judged as satisfied.	
SA-3: Critical Data Misperceived	Yes	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.	16
SA-4: Critical Data Dismissed/Discounted	No	The level criterion is below what could be expected in a normal reactor trip situation.	
SA-5: Premature Termination of Critical Data Collection	No	The STA will periodically check the CSFST.	
RP-1: Misinterpret Procedures	No	Simple transfer with no further decision required.	
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
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	Not an execution step	

Table C-25 Evaluation of CFM AP-2 for HFE 2, Critical Task 3

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	**Assessment**	**Justification**
Workload	Low	Nominal workload
Procedure	Simple	Procedure is straightforward.
Compensatory Factors	N/A	
Recovery Potential	Yes	
Crew Failure Scenario #		14

Table C-26 Evaluation of CFM SA-3 for HFE 3, Critical Task 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. 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	Yes	
Crew Failure Scenario #		16

C.2.4.4 Critical Task 4

Table C-27 CFM Selection Table for HFE 2, Critical Task 4

CRD Node	5		
Critical Task	4		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	No alarm	
AP-2: Misread or Skip Critical Step(s) in Procedure*	No	N/A. Execution step.	

SA-1: Data Misleading or Not Available	No	N/A. Execution step.	
SA-2: Wrong Data Source Attended To	No	N/A. Execution step.	
SA-3: Critical Data Misperceived	No	N/A. Execution step.	
SA-4: Critical Data Dismissed/Discounted	No	N/A. Execution step.	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	No	Procedure is clear	
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	Yes	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.	7
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
E-3: Fail to Initiate Execution	No	At this stage the crew is focused on the F&B as its immediate priority.	
E-4: Fail to Correctly Execute Response (Simple Task)	Yes	Simple manipulation. It consists two tasks: SI actuation and establishing a bleed path. Other intermediate steps are to verify the effectiveness of the actions	6
E-5: Fail to Correctly Execute Response (Complex Task)	No	Simple manipulation	

* CFM AP-2 was identified as applicable for Critical Task 4 in the original analysis.

Table C-28 Evaluation of CFM E-1 for HFE 2, Critical Task 4

E-1: Delay Implementation		
PIF	**Assessment**	**Justification**
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	
Crew Failure Scenario #		7

Table C-29 Evaluation of CFM E-2 for HFE 2, Critical Task 4

E-4: Fail to Correctly Execute Response (Simple Task)		
PIF	**Assessment**	**Justification**
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.
Crew Failure Scenario #		6

C.2.5 Summary of Analysis

This scenario is complicated by the misleading AFW flow indication due to mis-positioned AFW recirculation valve. The procedure and the CSFSTs do not address the valve or allow for prompt diagnosis of loss of heat sink. The only path to initiate F&B is via in this scenario, and the only direct path that will instruct entry into FRH1 is via the heat sink CSFST. However, the tree will show a yellow rather than red path.

The crew will enter ES01 at E0 Step 4 since SI is neither actuated nor required. Criteria to enter FRH1 are not part of ES01. The Conditional Information Page for ES01 and the steps of ES-01 do not include any condition for transferring to FRH1. Thus, the decision to transfer to FRH1 is based on evaluation of the heat sink CSFST in parallel with the execution of ES01 steps.

Several factors can help the crew realize the entry condition of FRH1 is actually met.

First, the crew is trained on loss of main feedwater with mis-positioned AFW recirculation valves at least once every two years, and the plant had an operating experience of AFW recirculation valves being mis-positioned years ago. When they leave E0, the crew will monitor feed flow and check AFW status by looking at multiple indications, including the SG tank levels. The SG levels will initially fall after the reactor trip. With a feed flow of 576 GPM, they are expected to come back on scale (NR) within five minutes. However, the level will continue to drop in this case. If the SG levels do not return and keep trending down with indicated AFW flow, the crew will realize that there is a problem with the AFW and then verify AFW flow with the AFW tank level on the plant computer, which will take about 30 seconds.

Second, Step 3 of ES01 will instruct the crew to check feedwater flow. It takes 3 minutes to reach Step 3 after entry of ES01.

Third, the STA is likely to be called at the beginning of this scenario and be active when the crew starts to monitor critical safety functions and reaches ES01 Step 3. One of the STA's responsibilities is to monitor the Critical Safety Functions (CSFs). Once the AFW flow problem is brought into attention, he or she will look at the AFW tank level to recognize that the criteria to start FRH1 are met.

After the crew enters FRH1, the crew will be guided to decide to initiate F&B by Step 2 by checking SG levels. The implementation will not be challenging due to training. However, the crew may experience some time pressure as they are told to implement F&B quickly.

Recovery analysis:

There are multiple indications and procedural steps for potential recovery. The time is sufficient for recovery.

Table C-30 HEP Calculation Table for HFE 2

CRD Node #	Critical Task #	CFM	Crew Failure Scenario #	HEP
3	1	SA-2: Wrong Data Source Attended To	16	5.2E-05
		SA-3: Critical Data Misperceived	16	1.3E-05
3	2	SA-1: Data Misleading or Not Available	5	9.6E-03
4	3	AP-2: Misread or Skip Critical Step(s) in Procedure	14	1.2E-04
		SA-3: Critical Data Misperceived	16	1.3E-05
5	4	E-1: Delay Implementation	7	1.7E-05
		E-4: Fail to Correctly Execute Response (Simple Task)	6	1.6E-06
			Total HEP:	**9.8E-03**

* CFM AP-2 was identified as applicable for Critical Task 4 in the original analysis. It was deleted from this analysis because CFM AP-2 is not applicable to execution tasks.

As shown in Table C-30~~Table C-30~~, there is no specific negative PIF. The misleading indication is compensated by training and other confirmatory indications.

C.3 Human Failure Event 3

C.3.1 PRA Scenario Description, Expected Operator Response and HFE Definition

This scenario is adapted from an actual event. See Scenario Descriptions for detailed information on sequence of key events.

Plant technical information:

- 3-loop Westinghouse pressurized water reactor (PWR)
- There are two main feedwater (FW) pumps: A and B
- There are three charging pumps: A, B and C
- There are three component cooling water (CCW) pumps: A, B and C

Situation from start:

- The plant is operating in Mode 1 at approximately 100% power.
- The Shift Manager and Shift Technical Advisor are outside of the control room at a shift turnover meeting.

- CCW Pump C and Charging Pumps A and C are running.
- FW Pumps A and B are running.

Event overview:

At 18:52 with the plant operating in Mode 1 at approximately 100% power, an electrical feeder cable failure caused an arc flash and fire on a non-vital electrical bus. The electrical bus failed to isolate due to a breaker failure, and the fault persisted much longer than design expectations. The effects were widespread throughout the electrical systems. The electrical isolations and automatic repowering also created time sequences that caused inadvertent equipment actuation and damage. The fault condition reduced voltage to Reactor Coolant Pump (RCP) B, causing an automatic reactor trip on Reactor Coolant System (RCS) loop low flow. Pressurizer level and pressure decreased due to RCS cooldown, resulting in an automatic safety injection (SI). Plant response was further complicated by multiple equipment malfunctions.

Loss of RCP seal injection and cooling:

Within the first minute of the initiating event, RCP seal cooling (via Component Cooling Water (CCW)) is lost due to the closing of Flow Control Valve (FCV) 626, the component cooling water thermal barrier outlet isolation valve. FCV-626 closed due to an inaccurate high-flow signal when the flow sensor lost power during electrical realignments resulting from the fault.

Approximately 27 minutes into the event, Chemical and Volume Control (CVC) Valve 310A fails open. When CVC-310A fails open the charging flow is diverted from the RCP seals to the RCS and RCP seal injection becomes inadequate (there is some injection flow, but it is inadequate to fulfill its safety function). As a result, the RCP seals begin to heat up and purge volume begins to empty.

Figure C-10~~Figure C-10~~ is the event tree with the sequence highlighted.

Expected operator response:

With both RCP seal cooling from CCW unavailable and seal injection inadequate, the appropriate crew response would be to restore seal cooling from CCW to the RCP thermal barrier heat exchangers.

For successful recovery, operators would have to re-open FCV-626 from the control room before voiding within the RCPs occurs (see Figure C-11~~Figure C-11~~). Based on Westinghouse calculations, the RCP seals will experience voiding conditions approximately 19 minutes after all RCP seal cooling and injection are lost.

HFE definition:

Failure to restore CCW to the RCP thermal barrier heat exchangers by re-opening FCV-626.

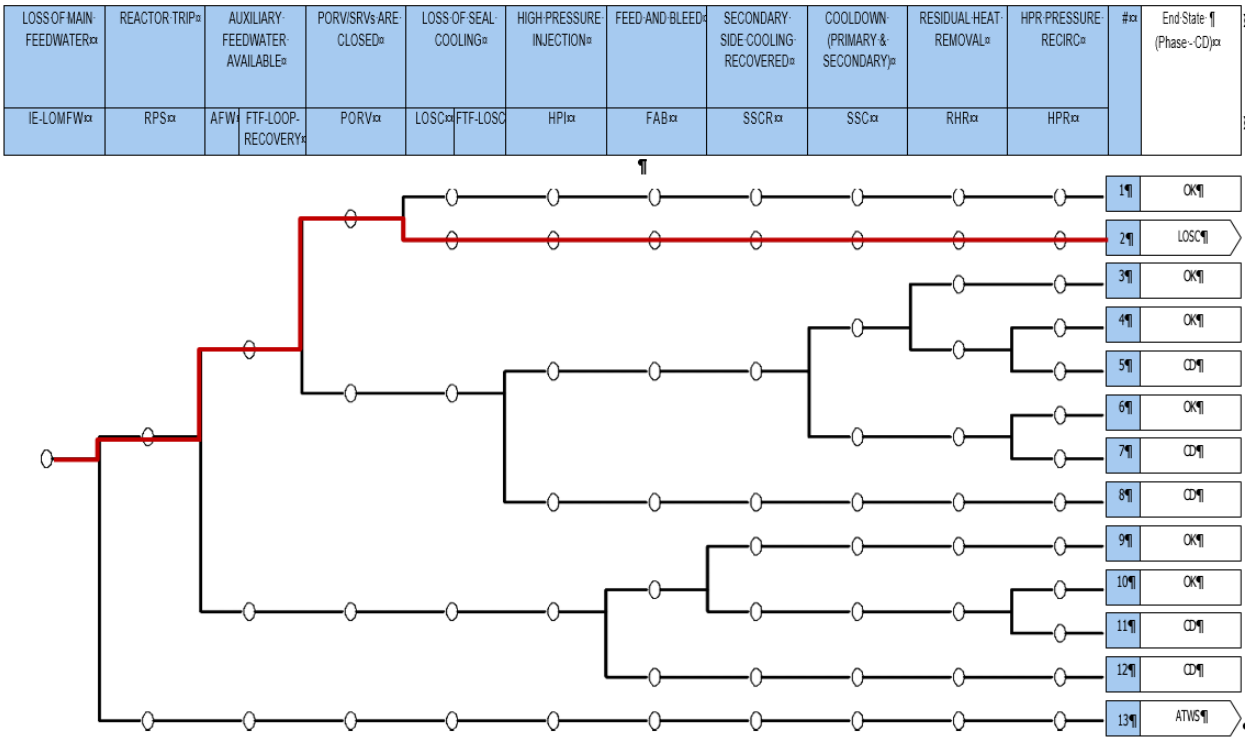


Figure C-10 Loss of Main Feedwater Event Tree for HFE 3

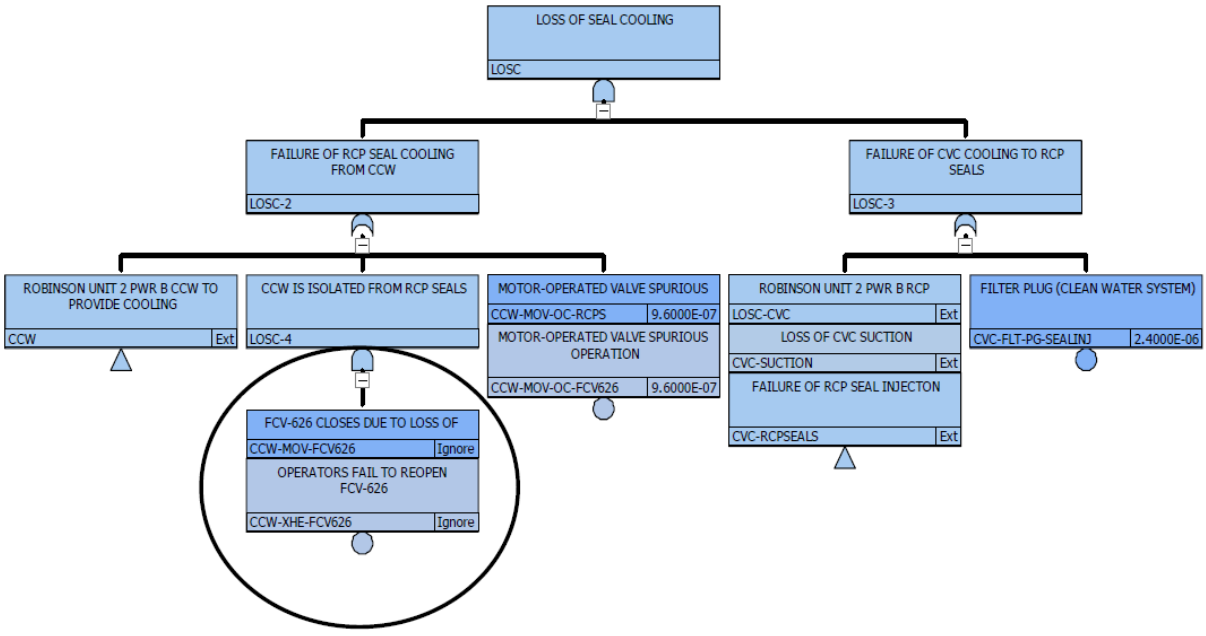


Figure C-11 Loss of Seal Cooling Fault Tree for HFE 3

C.3.2 Crew Response Diagram (CRD) and Task Analysis

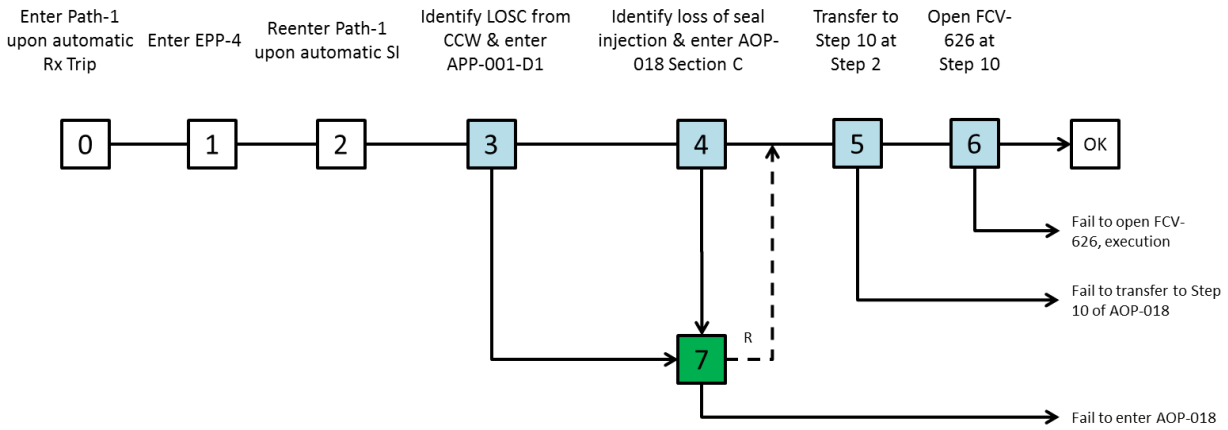


Figure C-12 Crew Response Diagram for HFE 3

C.3.2.1 Node 0: Enter Path-1 upon automatic reactor trip

The crew enters Path-1 (Emergency Procedure Flow Path) upon automatic reactor trip at 18:52. Success is assumed as this is a highly trained crew response. This node is for information only and there are no critical tasks associated with it.

C.3.2.2 Node 1: Enter EPP-4

The crew enters End Path Procedure (EPP) 4, Reactor Trip Response from Path-1 when they decide no SI is required. This node is an HFE boundary condition event as defined in the scenario description. There are no critical tasks associated with it.

C.3.2.3 Node 2: Reenter Path-1 upon automatic SI

The crew reenters Path-1 at 19:00 upon automatic SI due to a rapid cooldown. At this point, only one charging pump (Pump B) is running. CCW Pump B and Pump C are running, however; CCW cannot reach RCP seal because FCV-626 is closed.

This node is an HFE boundary condition event as defined in the scenario description. There are no critical tasks associated with it.

C.3.2.4 Node 3: Identify loss of seal cooling (LOSC) from CCW & enter APP-001-D1

One step in Path-1 will direct the crew to check the RCP Thermal Barrier Cooling Water Low Flow Annunciator (see the highlighted diamond step in Figure C-13~~Figure C-13~~). This provides an opportunity for them to recognize LOSC from CCW due to the closure of FCV-626.

According to the scenario description, this annunciator is annunciated when FCV-626 closes at 18:52. However, many systems or components fail or become unavailable due to the electrical fault. Workload is expected to be extremely high (see attached Workload Assessment Table) at

the beginning of the scenario – the crew is busy with reactor trip, SI, and responding to the fire at the same time, especially when the BOP is dedicated to AOP-041, Response to Fire Event, for about 40 minutes. Therefore, the crew will either not notice the RCP Thermal Barrier Cooling Water Low Flow Annunciator or ignore it. The crew will ignore the alarm because restoring seal cooling from CCW is not their priority at the beginning of the scenario, given that the crew has started Charging Pumps B and C per Path-1 to restore RCP seal injection at 18:53. Even when SI is automatically actuated at 19:00, Charging Pump B is still running, providing adequate seal injection.

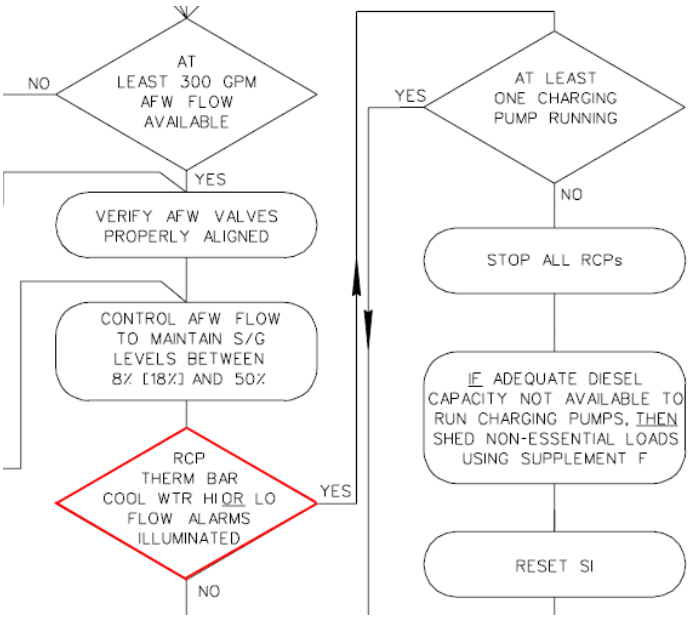


Figure C-13 Procedural step in Path-1 to check the RCP Thermal Barrier Cooling Water Low Flow Annunciator for HFE 3

Seal injection becomes inadequate when CVC-310A fails fully open at 19:19. The crew will reach the diamond step in Figure C-13~~Figure C-13~~ about 30 minutes after the reactor trip (i.e., 19:22). As such, when the crew reaches the step, seal injection becomes inadequate and restoring seal cooling becomes important.

Whether the crew will enter Annunciator Panel Procedure APP-001-D1 to respond to the RCP Thermal Barrier Cooling Water Low Flow Annunciator depends on whether the crew has enough manpower. At this point, the plant has come to a relatively more stable state compared to the beginning of the scenario as distractions die down. Although the BOP is still dedicated to AOP-041 and workload is still considered higher than normal (see attached Workload Assessment Table), workload becomes relatively lower so that the crew has enough manpower to enter APP-001-D1 while they continue in Path-1, which is an assumption based on discussion with plant staff.

The critical tasks associated with Node 3 include:

- Check the RCP Thermal Barrier Cooling Water Low Flow Annunciator per the diamond step in Path-1

C.3.2.5 Node 4: Identify loss of seal injection & enter AOP-018 Section C

Step 4 of APP-001-D1 is listed below.

Step 4:

IF FCV-626 has failed closed, THEN PERFORM the following:

1) VERIFY RCP Seal Injection flow 6gpm to 20 gpm.

2) ATTEMPT to reopen FCV-626

3) IF FCV-626 will NOT reopen, THEN INITIATE action to restore FCV-626 to OPERABLE status and CONTACT Engineering for assistance.

At Sub-step 1, the crew can look at seal injection trend to check RCP seal injection flow rate. At this point, CVC-310A has failed fully open and seal injection is below 6gpm, which is deemed as inadequate. This is a cue for the crew to realize loss of seal injection and then enter Abnormal Operating Procedure AOP-018 (Reactor Coolant Pump Abnormal Conditions) without opening FCV-626. AOP-018 has three sections, and Section C addresses loss of seal injection. Transferring to Section C is assumed success given training and the fact that the crew entered AOP-018 based on their diagnosis of loss of seal injection.

<u>The critical tasks associated with Node 4 include:</u>

- Verify RCP seal injection flow rate between 6 and 20 gpm

C.3.2.6 Node 5: Transfer to Step 10 at Step 2

Step 2 and its RNO column of Section C of AOP-018 is listed below.

Step 2:

Check Elapsed Time Since All RCP Seal Cooling Was Lost – GREATER THAN 15 MINUTES

Step 2 RNO:

IF RCP Seal Cooling is NOT OR can NOT be restored in less than 15 minutes. THEN Go To Step 3.

Go To Step 10.

At Step 2, the crew will look at seal injection trend to determine how long seal injection has been lost. The seal injection becomes inadequate at 19:19. The crew enters APP-001-D1 around 19:22. It will take them about 1 minute to check RCP seal injection flow rate, 2 minutes to transfer to Section C of AOP-018 from APP-001-D1 (i.e., 19:25), and 1 minute to reach Step 2 (i.e., 19:26). That is, 7 minutes has elapsed since all RCP seal cooling was lost when the crew check the elapsed time at Step 2. Therefore, the crew will go to Step 2 RNO and then transfer to Step 10 since there is no indication for them to believe that RCP Seal Cooling cannot be restored in less than 15 minutes.

If the crew does not transfer to Step 10 at Step 2, the crew will be instructed to close FCV-626 at Step 5.

The critical tasks associated with Node 4 include:

- Check elapsed time since all RCP Seal Cooling was Lost

C.3.2.7 Node 6: Open FCV-626 at Step 10

Step 10 of Section C of AOP-018 is the procedural direction for opening FCV-626. It takes 1 minute to transfer to Step 10 and 1 minute to open FCV-626 (i.e., 19:28). Thus, the RCP seal cooling is restored within 15 minutes after it was lost.

The critical tasks associated with Node 4 include:

- Open FCV-626 at Step 10, which is a simple execution

C.3.2.8 Node 7: Recovery of Nodes 3 and 4

At Node 3, the crew may choose not to enter APP-001-D1 if there is not enough manpower. They may still think that restoring seal cooling from CCW is not priority because they are not aware that CVC-310A has failed open and seal injection has become inadequate. The step immediately after the diamond step (see Figure C-13~~Figure C-13~~ and discussion about Node 1) asks the crew to check if at least one charging pump is running. This step may reinforce the crew's decision that restoring seal cooling from CCW is not priority because Charging Pump B is providing sufficient seal injection. In this case, the crew, based on training, would enter Section C of AOP-018 upon RCP B and RCP A High Bearing Temperature Alarms, which occur at 19:24 and 19:30, respectively. Since it takes about 1 minute to enter Section C of AOP-018 and 3 minutes to open FCV-626 afterwards (see discussion about Nodes 5 and 6). The RCP seal cooling can be restored within 15 minutes after it was lost if the crew enters AOP-018 upon RCP B High Bearing Temperature Alarm at 19:24. However, if the crew enters AOP-018 upon RCP A High Bearing Temperature Alarm at 19:30, the crew needs to respond very fast to meet the 15-minute time window requirement.

At Node 4, the crew may fail to recognize loss of seal injection when they see seal injection flow rate is below 6gpm at APP-001-D1 Step 4. Similarly to recovery for Node 3, RCP B and RCP A High Bearing Temperature Alarms give the crew an opportunity to enter AOP-018. The crew is expected to enter APP-001-D1 at 19:22 and reach Step 4 at 19:26. By then, the RCP B High Bearing Temperature Alarm has been annunciated. The alarm, reinforced by the low seal injection flow, should make the crew realize loss of seal injection. If the crew miss both cues, RCP A High Bearing Temperature Alarm is another cue, but the crew needs to respond very fast to meet the 15-minute time window requirement.

C.3.2.9 Task Analysis

Table C-31 Task Analysis for HFE 3

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information
3	1	Check the RCP Thermal Barrier Cooling Water Low Flow Annunciator per the diamond step in Path-1	• Read and interpret the diamond step in Path-1 correctly • Identify the correct annunciator • Interpret the annunciator status • Make procedure transfer based on training	The annunciator is annunciated at the beginning of the scenario when FCV-626 is closed due to electrical failure. Assumptions made: • Enough manpower • Working in APP-001-D1 in parallel with Path 1.
4	2	Verify RCP seal injection flow rate between 6 and 20 gpm	• Identify correct data source (seal injection flow rate trend) • Interpret seal injection trend correctly (comparing against numerical criteria in procedure and realizing LOSC) • Make procedure transfer based on training	Seal injection trend is assumed to be available. Seal injection flow rate below 6gpm means loss of seal injection.
5	3	Check elapsed time since all RCP Seal Cooling was Lost	• Identify correct data source (seal injection flow rate trend) • Interpret seal injection trend to determine elapsed time • Correctly interpret procedure to transfer to Step 10	Seal injection trend is assumed to be available.
6	4	Open FCV-626 at Step 10, which is a simple execution	Simple execution from the control room	

C.3.3 Timeline

The timeline for HFE-3 is illustrated in Figure C-14~~Figure C-14~~. The green color represents actual events or boundary conditions, and the cyan color represents predicted events and estimates.

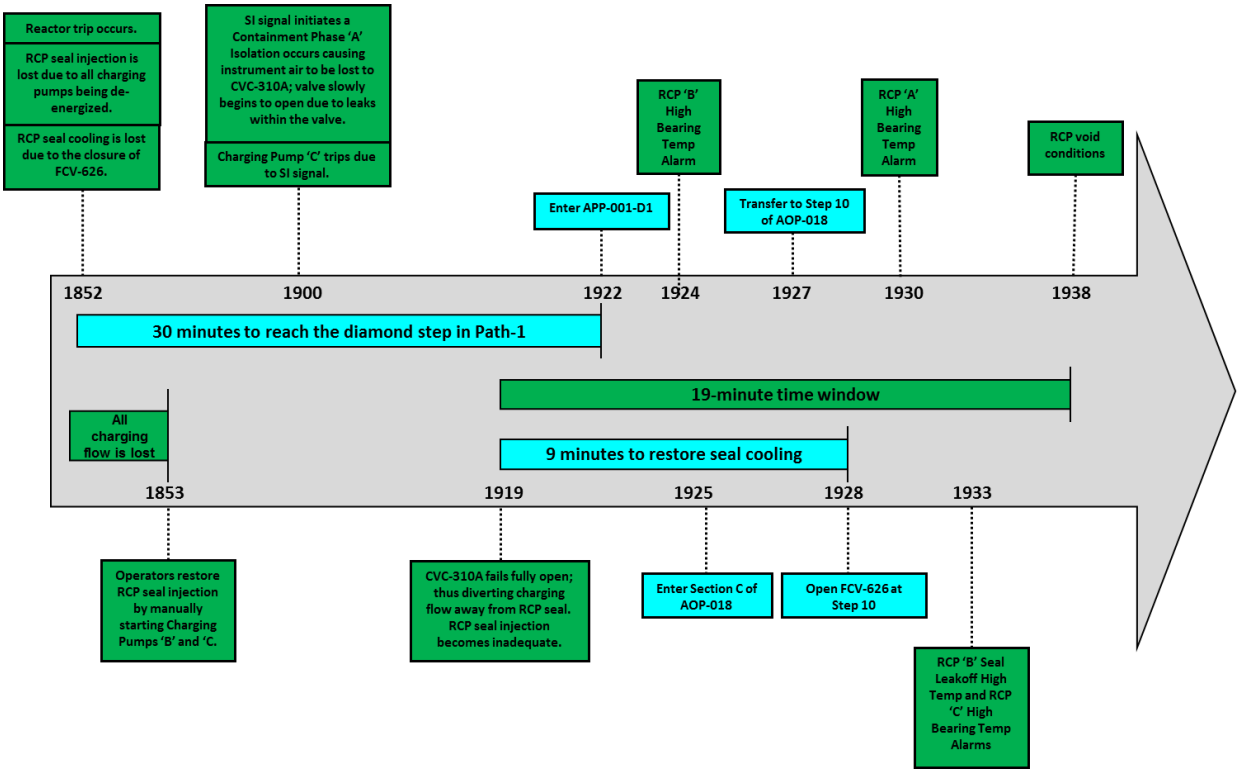


Figure C-14 Timeline for HFE 3

The following information was obtained through discussion with plant staff.

- It will take 30 minutes for the crew to reach the diamond step in Figure C-13~~Figure C-13~~ after the reactor trip (i.e., 19:22).
- It takes about 1 minute to check RCP seal injection flow rate at Step 4 of APP-001-D1.
- It takes about 2 minutes to transfer to Section C of AOP-018 from APP-001-D1 (i.e., 19:25).
- It takes about 1 minute to reach Step 2 after entry of Section C of AOP-018.
- It takes about 1 minute to transfer to Step 10 from Step 2.
- It takes about 1 minute to open FCV-626 at Step 10.

Per guidance of AOP-018, the crew need to open FCV-626 within 15 minutes after all seal cooling is lost, which is within the 19-minute window specified for HFE-3.

C.3.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees

C.3.4.1 Critical Task 1

Table C-32 CFM Selection Table for HFE 3, Critical Task 1

CRD Node	3		
Critical Task	1		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	Directed search by procedure.	
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	The crew may skip the diamond step in Path-1 due to high workload. The crew is working in two procedures.	8
SA-1: Data Misleading or Not Available	No	Instrumentation works properly and indications are available in the MCR.	
SA-2: Wrong Data Source Attended To	Yes	Potentially applicable	12
SA-3: Critical Data Misperceived	No	Nominal ergonomics. The annunciator is either lit or not.	
SA-4: Critical Data Dismissed/Discounted	No	The CFM is irrelevant because the crew is directed by the procedure to check the alarm. This critical task involves perception of the status of the annunciator.	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	Yes	Required response is not explicitly specified if the annunciator is lit.	4
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	No	Not an execution step	
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
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	Not an execution step	

Table C-33 Evaluation of CFM AP-2 for HFE 3, Critical Task 1

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	**Assessment**	**Justification**
Workload	High	The crew needs to respond to multiple failures. The BOP is dedicated to AOP-041. Although the workload is lower than that at the beginning of the scenario, it is expected to be higher than normal. The crew is working in two procedures.
Procedure	Simple	Path-1 is trained on frequently and straightforward.
Compensatory Factors	Present	
Recovery Potential	Yes	RCP B and RCP A High Bearing Temperature Alarms.
Crew Failure Scenario #		*8*

Table C-34 Evaluation of CFM SA-2 for HFE 3, Critical Task 1

SA-2: Wrong Data Source Attended to		
PIF	**Assessment**	**Justification**
HSI	Good	HSI is assumed to be nominal.
Workload	High	The crew needs to respond to multiple failures. The BOP is dedicated to AOP-041. Although the workload is lower than that at the beginning of the scenario, it is expected to be higher than normal. The crew is working in two procedures.
Familiarity with Data Source	Good	The crew is well trained on the data source.
Recovery Potential	Yes	RCP B and RCP A High Bearing Temperature Alarms.
Crew Failure Scenario #		*12*

Table C-35 Evaluation of CFM RP-1 for HFE 3, Critical Task 1

RP-1: Misinterpret Procedures		
PIF	**Assessment**	**Justification**
Procedures Open to Misinterpretation	Yes	The Path-1 step does not specify response if the alarm is annunciated.
Workload	High	The crew needs to respond to multiple failures. The BOP is dedicated to AOP-041. Although the workload is lower than that at the beginning of the scenario, it is expected to be higher than normal. The crew is working in two procedures.
Training/Experience	Good	Training on Path-1 is assumed to be good. The crew will work in APP-001-D1 in parallel with Path-1 if manpower is sufficient.
Recovery Potential	Yes	RCP B and RCP A High Bearing Temperature Alarms.
Crew Failure Scenario #		*4*

C.3.4.2 Critical Task 2

Table C-36 CFM Selection Table for HFE 3, Critical Task 2

CRD Node	4		
Critical Task	2		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	No alarm	
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	The crew may skip the step to check seal injection flow rate due to high workload. The crew is working in two procedures.	8
SA-1: Data Misleading or Not Available	No	Instrumentation works properly and indications are available in the MCR.	
SA-2: Wrong Data Source Attended To	No	Only one indication	
SA-3: Critical Data Misperceived	Yes	Comparison against numerical values specified in procedure. Misperception may be due to high workload. The crew is working in two procedures.	10
SA-4: Critical Data Dismissed/Discounted	No	N/A. There is not a valid alternative scenario.	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	Yes	Required response is not explicitly specified if the seal injection flow rate is below 6gpm.	2
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	No	Not an execution step	
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
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	Not an execution step	

Table C-37 Evaluation of CFM AP-2 for HFE 3, Critical Task 2

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	**Assessment**	**Justification**
Workload	High	The crew needs to respond to multiple failures. The BOP is dedicated to AOP-041. Although the workload is lower than that at the beginning of the scenario, it is expected to be higher than normal. The crew is working in two procedures.
Procedure	Simple	Procedure is straightforward.
Compensatory Factors	Present	
Recovery Potential	Yes	RCP B and RCP A High Bearing Temperature Alarms.
Crew Failure Scenario #		*8*

Table C-38 Evaluation of CFM SA-3 for HFE 3, Critical Task 2

SA-3: Critical Data Misperceived		
PIF	**Assessment**	**Justification**
HSI/Environment	*Good*	Nominal ergonomics.
Workload	*High*	The crew needs to respond to multiple failures. The BOP is dedicated to AOP-041. Although the workload is lower than that at the beginning of the scenario, it is expected to be higher than normal. The crew is working in two procedures.
Training	*Poor*	The POOR branch is chosen conservatively. The crew may be trained on APP-001-D1, but probably not specifically in the context of this scenario. More specifically, the crew may not be trained on the significance of this step when there is high workload and other potential competing tasks.
Recovery Potential	*Yes*	RCP B and RCP A High Bearing Temperature Alarms.
Crew Failure Scenario #		*10*

Table C-39 Evaluation of CFM RP-1 for HFE 3, Critical Task 2

RP-1: Misinterpret Procedures		
PIF	**Assessment**	**Justification**
Procedures Open to Misinterpretation	Yes	Required response is not explicitly specified if the seal injection flow rate is below 6gpm.
Workload	High	The crew needs to respond to multiple failures. The BOP is dedicated to AOP-041. Although the workload is lower than that at the beginning of the scenario, it is expected to be higher than normal. The crew is working in two procedures.

Training/Experience	LTA	The LTA branch is chosen conservatively given APP-001-D1 is an alarm response procedure. The crew may be trained on this procedure, but probably not specifically in the context of this scenario. More specifically, the crew may not be trained on the significance of this step when there is high workload and other potential competing tasks.
Recovery Potential	Yes	RCP B and RCP A High Bearing Temperature Alarms.
Crew Failure Scenario #		*2*

C.3.4.3 Critical Task 3

Table C-40 CFM Selection Table for HFE 3, Critical Task 3

CRD Node	5		
Critical Task	3		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	No alarm	
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable but unlikely.	13
SA-1: Data Misleading or Not Available	No	Instrumentation works properly and indications are available in the MCR.	
SA-2: Wrong Data Source Attended To	No	Only one indication	
SA-3: Critical Data Misperceived	Yes	Comparison against numerical values specified in procedure.	15
SA-4: Critical Data Dismissed/Discounted	No	N/A. There is not a valid alternative scenario.	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	No	Procedure is clear.	
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	No	Not an execution step	
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
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	Not an execution step	

Table C-41 Evaluation of CFM AP-2 for HFE 3, Critical Task 3

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	**Assessment**	**Justification**
Workload	Low	It is assumed that the crew is working only in AOP-018 except the BOP. While the general workload is higher than normal for the crew, low workload is applicable here because this relates to the workload of the operator who is working in AOP-018. This operator will focus on the tasks in this procedure only without additional workload or distractors.
Procedure	Simple	Procedure is straightforward.
Compensatory Factors	N/A	
Recovery Potential	No	
Crew Failure Scenario #		*13*

Table C-42 Evaluation of CFM SA-3 for HFE 3, Critical Task 3

SA-3: Critical Data Misperceived		
PIF	**Assessment**	**Justification**
HSI/Environment	*Good*	Nominal ergonomics.
Workload	*Low*	It is assumed that the crew is working only in AOP-018 except the BOP. While the general workload is higher than normal for the crew, low workload is applicable here because this relates to the workload of the operator who is working in AOP-018. This operator will focus on the tasks in this procedure only without additional workload or distractors.
Training	*Good*	Training on AOP-018 is assumed to be good.
Recovery Potential	*No*	
Crew Failure Scenario #		*15*

C.3.4.4 Critical Task 4

Table C-43 CFM Selection Table for HFE 3, Critical Task 4

CRD Node	6		
Critical Task	4		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	No alarm	

AP-2: Misread or Skip Critical Step(s) in Procedure*	No	N/A. Execution step.	
SA-1: Data Misleading or Not Available	No	N/A. Execution step.	
SA-2: Wrong Data Source Attended To	No	N/A. Execution step.	
SA-3: Critical Data Misperceived	No	N/A. Execution step.	
SA-4: Critical Data Dismissed/Discounted	No	N/A. Execution step.	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	No	Procedure is clear	
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	No	No apparent complicating factors to delay implementation.	
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
E-3: Fail to Initiate Execution	Yes	Applicable but unlikely. Procedural direction is to make sure FCV-626 is open.	5
E-4: Fail to Correctly Execute Response (Simple Task)	Yes	Simple manipulation	7
E-5: Fail to Correctly Execute Response (Complex Task)	No	Simple manipulation	

Table C-44 Evaluation of CFM E-3 for HFE 3, Critical Task 4

E-3: Fail to Initiate Execution		
PIF	**Assessment**	**Justification**
Immediacy	Yes	The crew is aware of LOSC. Thus, they will not hesitate to open FCV-626 when they find out the valve is closed per procedural direction.
Workload	N/A	
Recovery Potential	N/A	
Crew Failure Scenario #		*5*

Table C-45 Evaluation of CFM E-4 for HFE 3, Critical Task 4

E-4: Fail to Correctly Execute Response (Simple Task)		
PIF	**Assessment**	**Justification**
HSI	*Nominal/good*	Nominal ergonomics.

Workload	*Low*	It is assumed that the crew is working only in AOP-018 except the BOP. While the general workload is higher than normal for the crew, low workload is applicable here because this relates to the workload of the operator who is working in AOP-018. This operator will focus on the tasks in this procedure only without additional workload or distractors.
Recovery Potential	*No*	
Crew Failure Scenario #	*7*	

C.3.5 Summary of Analysis

This is a difficult and complex scenario. Many systems or components fail or become unavailable due to the electrical fault. Workload is expected to be extremely high at the beginning of the scenario because the crew needs to respond to many alarms and take care of the fire at the same time (see attached Workload Assessment Table). The BOP is dedicated to AOP-041, Response to Fire Event, for about 40 minutes. Workload may become relatively lower when the fire is under control and distractions die down, but it is expected to be higher than normal.

The crew will enter Path 1 upon reactor trip and then enter EPP-4 when they decide SI is not needed. However, they will reenter Path-1 when SI automatically initiates.

FCV-626 is closed at the beginning of the scenario and the RCP Thermal Barrier Cooling Water Low Flow Annunciator will be annunciated. The crew will probably not notice it given that many alarms will be annunciated at the beginning of the scenario. Even if the crew notice this alarm, they will probably ignore it because this is not their priority at this point given that one charging pump is running providing adequate seal injection. Note that the crew manually starts a charging pump to restore seal injection at the beginning of the scenario.

As the scenario progresses, the seal injection becomes inadequate when the VCT level decreases and CVC-310A fails open. However, the operator may not realize that and think there is adequate seal injection because at least one charging pump is running.

30 minutes after the initiating event, the crew will reach a step (see Figure C-13~~Figure C-13~~) in Path-1 to check the RCP Thermal Barrier Cooling Water Low Flow Annunciator. This is when they should realize there is no seal cooling from CCW. We choose to model this transition as Node 3 on the CRD. Whether they enter APP-001-D1 may depend on whether the crew has enough manpower to do so given the other responses being attended to. If the fire is under control, a crew member would be available to address APP-001-D1 while the rest of the crew continues in Path-1, which contributes to high workload. However, due to high workload, if for example the BOP is still working in AOP-041, Response to Fire Event, it is possible that the crew may not respond to the alarm at this step. One reason for this is that the operators may still think that there is enough seal injection as one charging pump is still running. Note that the step immediately after checking the RCP Thermal Barrier Cooling Water Low Flow Annunciator is to check if at least one charging pump is running.

If a crew member is given the responsibility to respond using APP-001-D1, then at step 4, he is told to check if the RCP seal injection flow is between 6gpm and 20gpm. At this point, the seal injection is below 6gpm because CVC-310A is fully open. Based on training, the crew should realize LOSC and then enter Section C of AOP-018 (Node 4).

At Step 2 of AOP-018, the crew will be asked to assess the elapsed time since all seal cooling is lost. The elapsed time should be less than 15 minutes. As a result, the crew will transfer to Step 10 to open FCV-626.

Recovery analysis:

If the crew fails to enter ADD-001-D1 at all at Node 3 or fails to recognize LOSC at Node 4, their only indication that seal cooling is inadequate is when they receive RCP bearing high temperature alarms. When these alarms occur, the crew is supposed to enter AOP-018 based on training. Due to the 15-minute time window, while RCP A High Bearing Temperature Alarm may be a recovery opportunity, it may not be viable.

Table C-46 HEP Calculation Table for HFE 3

CRD Node #	Critical Task #	CFM	Crew Failure Scenario #	HEP
3	1	AP-2: Misread or Skip Critical Step(s) in Procedure	8	1.5E-04
		SA-2: Wrong Data Source Attended To	12	3.2E-04
		RP-1: Misinterpret Procedures	4	5.3E-03
4	2	AP-2: Misread or Skip Critical Step(s) in Procedure	8	1.5E-04
		SA-3: Critical Data Misperceived	10	1.3E-04
		RP-1: Misinterpret Procedures	2	3.3E-02
5	3	AP-2: Misread or Skip Critical Step(s) in Procedure	13	8.2E-04
		SA-3: Critical Data Misperceived	15	1.3E-05
6	4	E-3: Fail to Initiate Execution	5	1.4E-04
		E-4: Fail to Correctly Execute Response (Simple Task)	7	9.3E-06
Total HEP:				**4.0E-02**

* CFM AP-2 was identified as applicable for Critical Task 4 in the original analysis. The total HEP is adjusted for deleting the CFM from the applicable CFMs for the critical task.

As shown in the table above, the significant contributors to the HEP are Nodes 3 and 4. Workload and procedure open to misinterpretation are dominating negative PIFs. Workload is considered high for Nodes 3 and 4 because the general workload is considered higher than normal and the crew is expected to work in two procedures. However, workload for Nodes 5 and 6 is considered low because it is assumed that most of the crew will focus on AOP-018 and will not have additional distractions.

Table C-47 Workload Assessment Table for HFE 3

Task context	Assessment / Basis	Outcome (Extremely high/ moderately high/ nominal)	Comment
Scenario familiarity			
Multitasking	One operator has to respond to fire. The crew has to work in both Path-1 and APP-001-D1	Extremely high	
Distraction / interruption	Many alarms. Fire may distract the crew, but one operator is dedicated to response to fire	High	
Dynamics predictability	Many systems or components fail or become unavailable due to the electrical fault. It's difficulty for the crew to perform plant assessment.	High	
Time pressure			
Timing			
Hours in work			

C.4 Human Failure Event 4

C.4.1 PRA Scenario Description, Expected Operator Response and HFE Definition

This scenario is adapted from an actual event. See Scenario Descriptions for detailed information on sequence of key events.

Plant technical information:

- 3-loop Westinghouse pressurized water reactor (PWR)
- There are two main feedwater (FW) pumps: A and B
- There are three charging pumps: A, B and C
- There are three component cooling water (CCW) pumps: A, B and C

Situation from start:

- The plant is operating in Mode 1 at approximately 100% power.
- The Shift Manager and Shift Technical Advisor are outside of the control room at a shift turnover meeting.
- CCW Pump C and Charging Pumps A and C are running.
- FW Pumps A and B are running.

Event overview:

At 18:52, with the plant operating in Mode 1 at approximately 100% power, an electrical feeder cable failure caused an arc flash and fire on a non-vital electrical bus. The electrical bus failed to isolate due to a breaker failure, and the fault persisted much longer than design expectations. The effects were widespread throughout the electrical systems. The electrical isolations and automatic repowering also created time sequences that caused inadvertent equipment actuation and damage. The fault condition reduced voltage to Reactor Coolant Pump (RCP) B, causing an automatic reactor trip on Reactor Coolant System (RCS) loop low flow. Pressurizer level and pressure decreased due to RCS cooldown, resulting in an automatic safety injection (SI). Plant response was further complicated by multiple equipment malfunctions.

Loss of RCP seal injection and cooling:

Within the first minute of the initiating event, RCP seal cooling (via Component Cooling Water (CCW)) is lost due to the closing of Flow Control Valve (FCV) 626, the component cooling water thermal barrier outlet isolation valve. FCV-626 closed due to an inaccurate high-flow signal when the flow sensor lost power during electrical realignments resulting from the fault.

Approximately 27 minutes into the event, Chemical and Volume Control (CVC) Valve 310A fails open. When CVC-310A fails open the charging flow is diverted from the RCP seals to the RCS and RCP seal injection becomes inadequate (there is some injection flow, but it is inadequate to fulfill its safety function). As a result, the RCP seals begin to heat up and purge volume begins to empty.

Figure C-15~~Figure C-15~~ is the LOMFW event tree with the sequence highlighted.

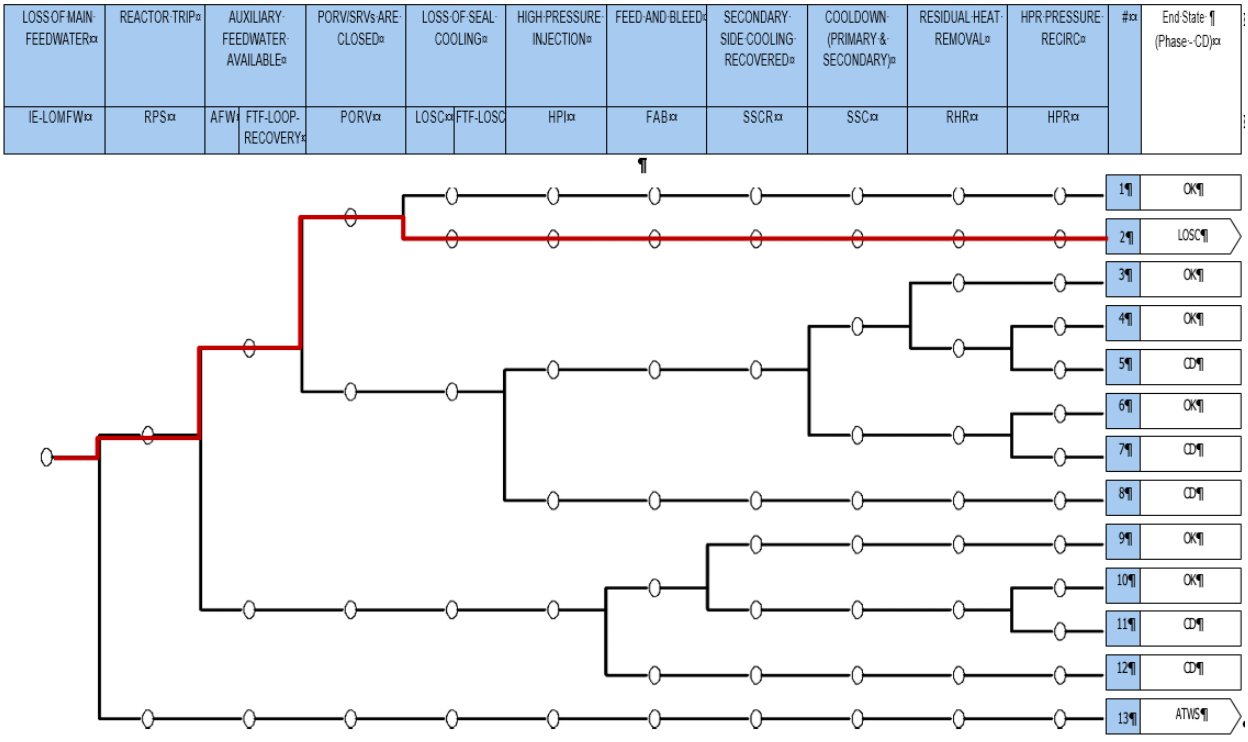


Figure C-15 Loss of Main Feedwater Event Tree for HFE 4

Expected operator response:

With both RCP seal cooling from CCW unavailable and seal injection inadequate, the appropriate crew response would be to restore seal cooling from CCW to the RCP thermal barrier heat exchangers.

For successful recovery, operators would have to re-open FCV-626 from the control room before voiding within the RCPs occurs (see Figure C-16~~Figure C-16~~).

If FCV-626 is not opened in time or cannot be opened, operators would need to trip the running RCPs prior to failure of the seals. RCP Pump B was tripped due to the loss of Bus 4 during the initial electrical fault. RCPs A and C remained running. Figure C-17~~Figure C-17~~ is the LOSC event tree with the sequence highlighted.

HFE definition:

Failure to trip the RCPs during a loss of all seal cooling and injection

Operators have approximately 19 minutes from when seal cooling and injection are lost to trip the running RCPs and avoid catastrophic seal failure (large enough to be equivalent to a small loss of coolant accident).

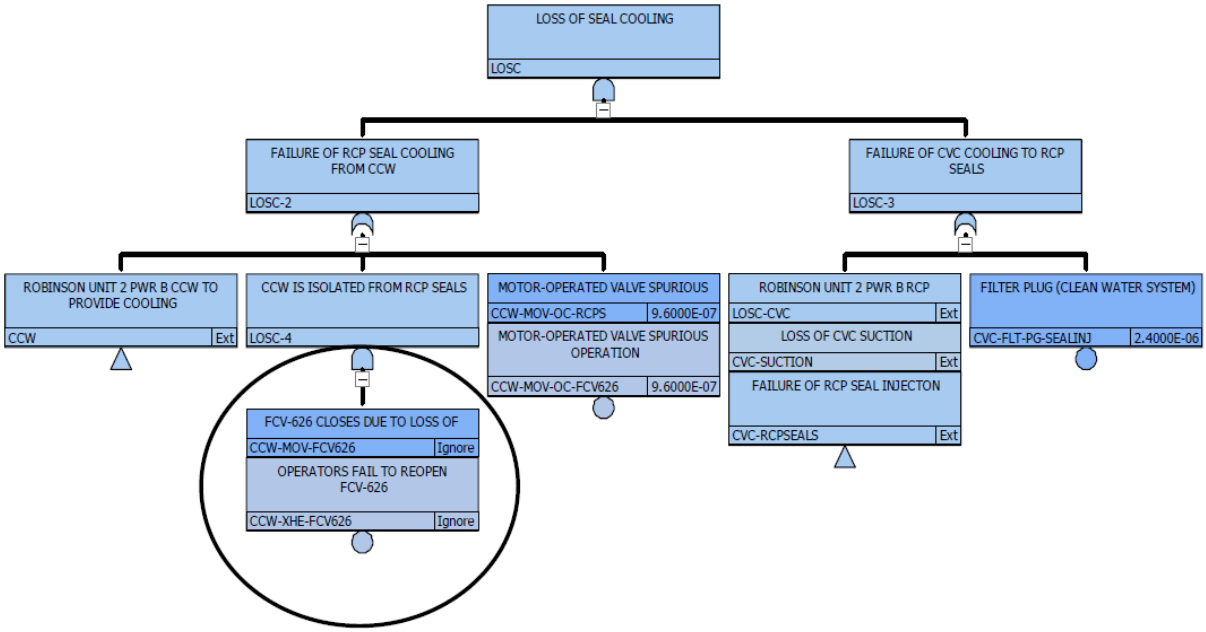


Figure C-16 Loss of Seal Cooling Fault Tree for HFE 4

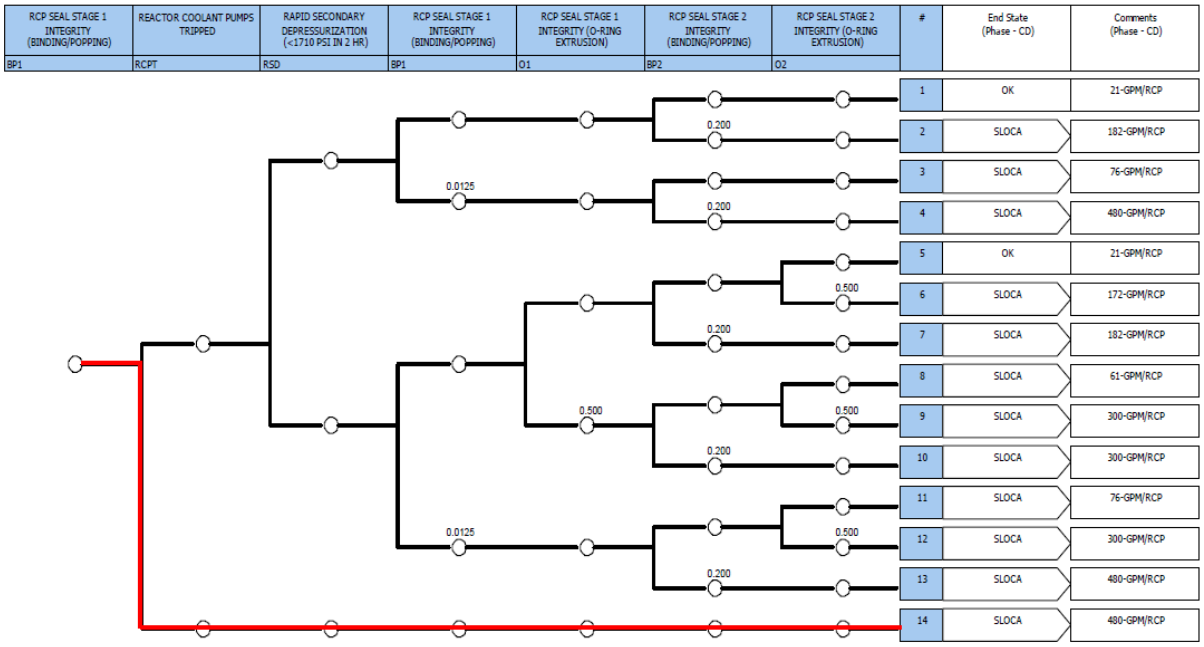


Figure C-17 Loss of Seal Cooling Event Tree for HFE 4

C.4.2 Crew Response Diagram (CRD) and Task Analysis

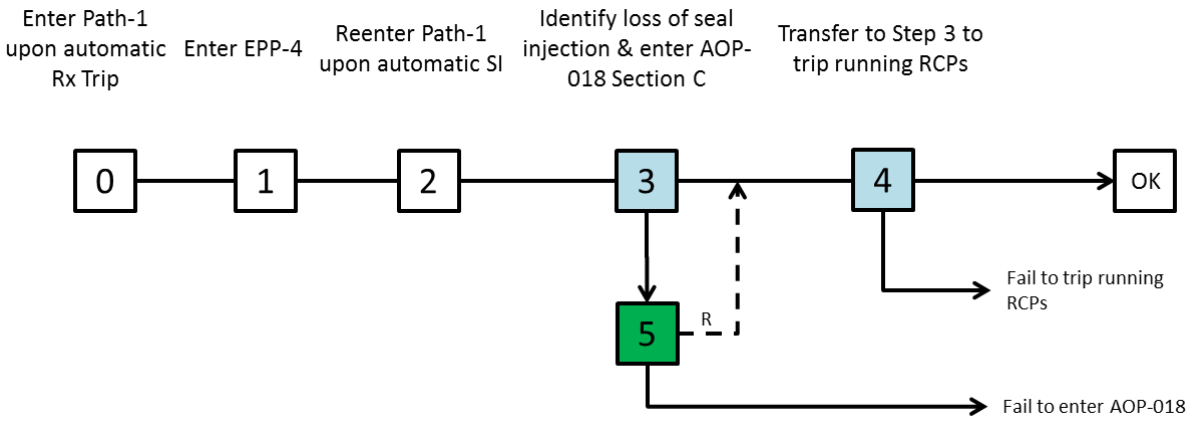


Figure C-18 Crew Response Diagram for HFE 4

C.4.2.1 Node 0: Enter Path-1 upon automatic reactor trip

The crew enters Path-1 (Emergency Procedure Flow Path) upon automatic reactor trip at 18:52. Success is assumed as this is a highly trained crew response. This node is for information only and there are no critical tasks associated with it.

1.1. Node 1: Enter EPP-4

The crew enters End Path Procedure (EPP) 4, Reactor Trip Response from Path-1 when they decide no SI is required. This node is an HFE boundary condition event as defined in the scenario description. There are no critical tasks associated with it.

C.4.2.2 Node 2: Reenter Path 1 upon automatic SI

The crew reenters Path-1 at 19:00 upon automatic SI due to a rapid cooldown. At this point, only one charging pump (Pump B) is running. CCW Pump B and Pump C are running, however; CCW cannot reach RCP seal because FCV-626 is closed. This node is an HFE boundary condition event as defined in the scenario description. There are no critical tasks associated with it.

C.4.2.3 Node 3: Identify loss of seal injection & enter Section C of AOP-018

Both Path-1 and Section C of AOP-018 provide guidance to trip the running RCPs. Path-1 directs the crew to trip RCPs if no charging pumps are running (see highlighted step in Figure C-19~~Figure C-19~~). The crew will reach this step about 31 minutes after the reactor is tripped (i.e., 19:23). At this point, seal injection has become inadequate -- CVC-310A fails fully open at 19:19. However, one charging pump is running and the crew is not aware that seal injection is diverted away through CVC-310A. In addition, cues of loss of seal injection have not occurred at this point (see discussion below). Therefore, the crew will not trip the RCPs per Path-1 without other indications of loss of seal injection.

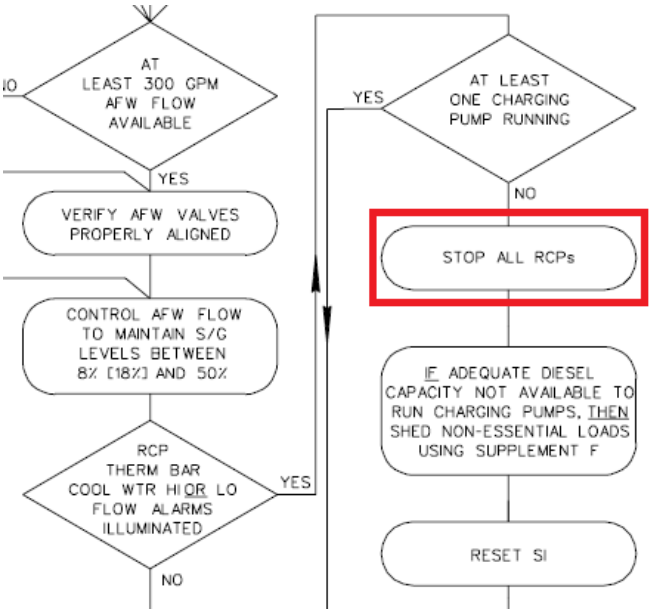


Figure C-19 Step in Path-1 to trip RCPs

The first cue for the crew to realize loss of seal injection is RCP B High Bearing Temperature Alarm at 19:24, which is one minute after the crew checks if at least charging pump is running in Path-1. This cue gives the crew 14 minutes to trip the RCPs. Based on training, the crew should enter Section C of AOP-018 when they receive this alarm. It will take 2 minutes to enter AOP-018 and transfer to Section C.

The critical tasks associated with Node 3 include:

- Attend to RCP B High Bearing Temperature Alarm and enter Section C of AOP-018

C.4.2.4 Node 4: Trip running RCPs at Step 3

The crew will enter Section C of AOP-018 around 19:26. It will take them about 1 minute to reach Step 2 (i.e., 19:27). As discussed above, the seal injection becomes inadequate at 19:19. Thus, 8 minutes has elapsed since all RCP seal cooling was lost when the crew reaches step 2, and they have 7 minutes to check the elapsed time and restore RCP seal cooling (i.e., 19: 34).

- If the crew decides at Step 2 that they cannot restore RCP seal cooling in 7 minutes, they will go to Step 3 to trip the RCPs.
- If they crew thinks that they can restore RCP seal cooling in 7 minutes, they will transfer to Step 10 and continue to other steps. (Note that although there is an opportunity to open FCV-626, we will assume that the valve will not be opened since this is an implicit assumption of HFE 4.) However, since Step 2 is a continuous step, the crew will monitor if they can restore RCP seal cooling in 15 minutes since all RCP seal cooling was lost. Once they decide that they cannot restore RCP seal cooling in 15 minutes, they will come back to Step 2 and then go to Step 3 to trip the RCPs.

In summary, the crew will need to transfer to Step 3 to trip the RCPs within 15 minutes since all RCP seal cooling was lost (i.e., 19:34) – it is just a matter of how the crew gets to Step 3. If we assume that the crew will transfer to Step 10 at Step 2, the crew will transfer back to Step 2 and then transfer to Step 3 at around 19:34. It takes another 1 minute to trip the RCPs at 19:35, which is within the 19-minute time window to avoid RCP void conditions.

Monitoring the time would be challenging for the crew given the fire and other distractions. The BOP operator will not be reintegrated with the crew until 19:32. (The BOP operation is dedicated to the fire procedure (AOP-041) from 18:52 through 19:32.) The crew may forget that Step 2 is a continuous step when they are progressing through the procedure. In addition, the crew might not check time with appropriate frequency when they are absorbed in other tasks in the procedure. Given that there is not much time for recovery, missing the 15-minute time window for several minutes will cause RCP void conditions.

Step 2 and its RNO column of Section C of AOP-018 is listed below.

Step 2:

Check Elapsed Time Since All RCP Seal Cooling Was Lost – GREATER THAN 15 MINUTES

Step 2 RNO:

IF RCP Seal Cooling is NOT OR can NOT be restored in less than 15 minutes. THEN Go To Step 3.

Go To Step 10.

Step 3 RNO of Section C of AOP-018 provides guidance to trip the running RCPs. Step 3 is listed below.

Step 3:

Check Plant Status – MODE 1 OR MODE 2

Step 3 RNO:

Stop the affected RCP(s)

Go To Step 5.

The critical tasks associated with Node 3 include:

- Decision to transfer to Step 3
- Trip running RCPs

C.4.2.5 Node 5: Recovery of Node 3

At Node 3, the crew may not notice RCP B High Bearing Temperature Alarm due to high workload and distractions. RCP A High Bearing Temperature Alarm at 19:30 and RCP B #1 Leak-off High Temperature and RCP C Bearing High Temperature Alarms at 19:33 will provide a recovery opportunity to realize loss of seal injection and then enter AOP-018. However, if the crew enters AOP-018 upon RCP B #1 Leak-off High Temperature and RCP C Bearing High Temperature Alarms, they need to act fast to meet the 19-minute time window.

C.4.2.6 Task Analysis

Table C-48 Task Analysis Table for HFE 4

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information
3	1	Attend to RCP B High Bearing Temperature Alarm and enter Section C of AOP-018	• Attend to the alarm • Interpret alarm correctly • Make procedure transfer based on training	It is assumed that the crew is well trained on entering AOP-018 upon RCP High Bearing Temperature Alarms.
4	2	Monitor elapsed time since all RCP seal cooling was lost	• Monitor time while trying to restore RCP seal cooling • Make procedure transfer correctly	High workload due to fire and other distractions. The BOP operator is dedicated to the fire procedure (AOP-041) from 18:52 through 19:32.) The crew may forget that Step 2 is a continuous step when they are progressing through the procedure. The

				crew might not check time with appropriate frequency when they are absorbed in other tasks in the procedure.
4	3	Trip running RCPs	• Read and interpret procedure correctly • Execute procedure instruction without delay and correctly	

C.4.3 Timeline

The timeline for HFE-4 is illustrated in Figure C-20~~Figure C-20~~. The green color represents actual events or boundary conditions, and the cyan color represents predicted events and estimates.

The following information was obtained through discussion with plant staff.

- It will take 31 minutes for the crew to reach the highlighted step in Figure C-19~~Figure C-19~~ after the reactor trip (i.e., 19:23).
- It takes about 2 minutes to enter AOP-018 and transfer to Section C after RCP B High Bearing Temperature Alarm (i.e., 19:26).
- It takes 15 minutes to reach Step 3 after entry of Section C of AOP-018 and then 1 minute to trip the RCPs.

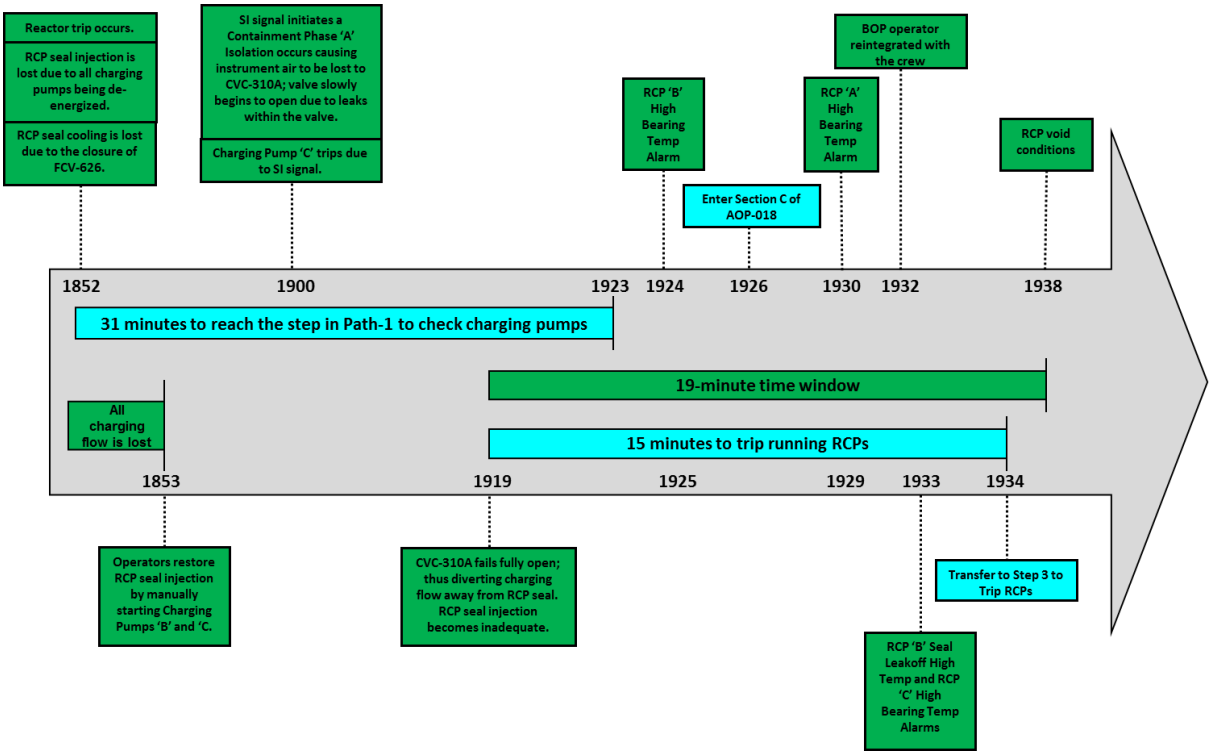


Figure C-20 Timeline for HFE 4

C.4.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees

C.4.4.1 Critical Task 1

Table C-49 CFM Selection Table for HFE 4, Critical Task 1

CRD Node	3		
Critical Task	1		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	Yes	High workload caused by fire and multiple failures.	4
AP-2: Misread or Skip Critical Step(s) in Procedure	No	Irrelevant. The crew just enters Section C of AOP-018.	
SA-1: Data Misleading or Not Available	No	Instrumentation works properly and indications are available in the MCR.	
SA-2: Wrong Data Source Attended To	No	Not directed search.	
SA-3: Critical Data Misperceived	No	Nominal ergonomics. The alarm is lit. No apparent reasons to misperceive.	
SA-4: Critical Data Dismissed/Discounted	Yes	But no valid alternative scenario	16
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	No	Irrelevant. The crew just enters Section C of AOP-018.	
RP-2: Choose Inappropriate Strategy	No	Irrelevant. The crew just enters Section C of AOP-018.	
E-1: Delay Implementation	No	Not an execution step	
E-2: Critical Data Not Checked/ Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
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	Not an execution step	

Table C-50 Evaluation of CFM AP-1 for HFE 4, Critical Task 1

AP-1: Key Alarm Not Attended To		
PIF	**Assessment**	**Justification**
Cognitive Workload/Distraction	*High*	The crew needs to respond to multiple failures. The BOP is dedicated to AOP-041. Although the workload

		is lower than that at the beginning of the scenario, it is expected to be higher than normal.
HSI	*Good*	Nominal ergonomics.
Perceived Urgency/Significance	*High*	The crew is trained on the RCP alarms.
Crew Failure Scenario #		*4*

Table C-51 Evaluation of CFM SA-4 for HFE 4, Critical Task 1

SA-4: Critical Data Dismissed/Discounted		
PIF	**Assessment**	**Justification**
Valid Alternative/ Deviation Scenario	*No*	
Inappropriate Bias	*N/A*	
Indications Reliable	*N/A*	
Confirmatory Information	*N/A*	
Recovery Potential	*N/A*	
Crew Failure Scenario #		*16*

C.4.4.2 Critical Task 2

Table C-52 CFM Selection Table for HFE 4, Critical Task 2

CRD Node	4		
Critical Task	2		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	No alarm involved.	
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	The crew may misread or skip Step 2. The crew may also forget that Step 2 is a continuous action when they are progressing through procedures.	7
SA-1: Data Misleading or Not Available	No	The crew is monitoring time.	
SA-2: Wrong Data Source Attended To	No	Not directed search. The crew is monitoring time rather than attending to a data source.	
SA-3: Critical Data Misperceived	Yes	The crew may misperceive time due to high workload.	11
SA-4: Critical Data Dismissed/Discounted	No	No valid alternative scenario.	

SA-5: Premature Termination of Critical Data Collection	No	No other viable plant status believable	
RP-1: Misinterpret Procedures	No	The procedure is clear.	
RP-2: Choose Inappropriate Strategy	No	Irrelevant.	
E-1: Delay Implementation	No	Not an execution step	
E-2: Critical Data Not Checked/ Monitored with Appropriate Frequency	Yes	The crew might not check time with appropriate frequency when they are absorbed in other tasks in the procedure.	3
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	Not an execution step	

Table C-53 Evaluation of CFM AP-2 for HFE 4, Critical Task 2

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	**Assessment**	**Justification**
Workload	High	When the crew enters AOP-018, the BOP is dedicated to the fire procedure (AOP-041) until 19:32. The rest of the crew will need to monitor time while continuing in AOP-018. The crew may forget that Step 2 is a continuous Step when they are absorbed in other tasks in the procedure.
Procedure	Simple	Procedure is straightforward.
Compensatory Factors	Present	Assuming nominal work practice and training.
Recovery Potential	No	
Crew Failure Scenario #		*7*

Table C-54 Evaluation of CFM SA-3 for HFE 4, Critical Task 2

SA-3: Critical Data Misperceived		
PIF	**Assessment**	**Justification**
HSI/Environment	*Good*	Assuming nominal HSI
Workload	*High*	When the crew enters AOP-018, the BOP is dedicated to the fire procedure (AOP-041) until 19:32. The rest of the crew will need to monitor time while continuing in AOP-018.
Training	*Good*	Assuming nominal work practice and training.
Recovery Potential	*No*	
Crew Failure Scenario #		*11*

Table C-55 Evaluation of CFM E-2 for HFE 4, Critical Task 2

E-2: Critical Data not Checked/Monitored with Appropriate Frequency		
PIF	**Assessment**	**Justification**
Monitoring Optimized	*No*	When the crew enters AOP-018, the BOP is dedicated to the fire procedure (AOP-041) until 19:32. The rest of the crew will need to monitor time while continuing in AOP-018.
Importance of Data Understood	*No*	Procedure does not tell the crew to prioritize monitoring time.
Match Expectations	*Good*	Assuming nominal training.
Alarm	*No*	
Crew Failure Scenario #		*3*

C.4.4.3 Critical Task 3

Table C-56 CFM Selection Table for HFE 4, Critical Task 3

CRD Node	4		
Critical Task	3		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	No alarm	
AP-2: Misread or Skip Critical Step(s) in Procedure*	No	N/A. Execution step.	
SA-1: Data Misleading or Not Available	No	N/A. Execution step.	
SA-2: Wrong Data Source Attended To	No	N/A. Execution step.	
SA-3: Critical Data Misperceived	No	N/A. Execution step.	
SA-4: Critical Data Dismissed/Discounted	No	N/A. Execution step.	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	No	Procedure is clear	
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	No	No apparent complicating factors to delay implementation. Only action in the queue.	
E-2: Critical Data Not Checked/ Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	

E-3: Fail to Initiate Execution	Yes	Applicable but unlikely. Procedural direction is to trip RCPs, which is the only action in the queue.	5
E-4: Fail to Correctly Execute Response (Simple Task)	Yes	Simple manipulation	7
E-5: Fail to Correctly Execute Response (Complex Task)	No	Simple manipulation	

Table C-57 Evaluation of CFM E-3 for HFE 4, Critical Task 3

E-3: Fail to Initiate Execution		
PIF	**Assessment**	**Justification**
Immediacy	Yes	The crew is aware of loss of seal injection. Thus, they will not hesitate to trip RCPs, which is the only action in the que.
Workload	N/A	
Recovery Potential	N/A	
Crew Failure Scenario #	*5*	

Table C-58 Evaluation of CFM E-4 for HFE 4, Critical Task 3

E-4: Fail to Correctly Execute Response (Simple Task)		
PIF	**Assessment**	**Justification**
HSI	*Nominal/good*	Nominal ergonomics.
Workload	*Low*	It is assumed that the crew is working only in AOP-018 except the BOP. While the general workload is higher than normal for the crew, low workload is applicable here because this relates to the workload of the operator who is working in AOP-018. This operator will focus on the tasks in this procedure only without additional workload or distractors.
Recovery Potential	*No*	
Crew Failure Scenario #	*7*	

C.4.5 Summary of Analysis

This is a difficult and complex scenario. Many systems or components fail or become unavailable due to the electrical fault. Workload is expected to be extremely high at the beginning of the scenario because the crew needs to respond to many alarms and take care of the fire at the same time (see attached Workload Assessment Table). The BOP is dedicated to AOP-041, Response to Fire Event, for about 40 minutes. Workload may become relatively lower when the fire is under control and distractions die down, but it is expected to be higher than normal.

The crew will enter Path 1 upon reactor trip and then enter EPP-4 when they decide SI is not needed. However, they will reenter Path-1 when SI automatically initiates.

Both Path-1 and Section C of AOP-018 provide guidance to trip the running RCPs. Path-1 directs the crew to trip RCPs if no charging pumps are running (see highlighted step in Figure C-19~~Figure C-19~~). The crew will reach this step about 31 minutes after the reactor is tripped (i.e., 19:23). At this point, seal injection has become inadequate -- CVC-310A fails fully open at 19:19. However, one charging pump is running and the crew is not aware that seal injection is diverted away through CVC-310A. In addition, cues of loss of seal injection have not occurred at this point (see discussion below). Therefore, the crew will not trip the RCPs per Path-1 without other indications of loss of seal injection.

The first cue for the crew to realize loss of seal injection is RCP B High Bearing Temperature Alarm at 19:24, which is one minute after the crew checks if at least charging pump is running in Path-1. This cue gives the crew 14 minutes to trip the RCPs. Based on training, the crew should enter Section C of AOP-018 when they receive this alarm. Step 3 will ask the crew to trip running RCPs. It takes about 5 minutes to trip the RCPs after the crew receives RCP B High Bearing Temperature Alarm or 10 minutes after seal injection becomes inadequate, which is within the 19-minute time window.

Recovery analysis:

At Node 3, the crew may not notice RCP B High Bearing Temperature Alarm due to high workload and distractions. RCP A High Bearing Temperature Alarm at 19:30 and RCP B #1 Leak-off High Temperature and RCP C Bearing High Temperature Alarms at 19:33 will provide a recovery opportunity to realize loss of seal injection and then enter AOP-018. However, if the crew enters AOP-018 upon RCP B #1 Leak-off High Temperature and RCP C Bearing High Temperature Alarms, they need to act fast to meet the 19-minute time window.

Table C-59 HEP Calculation Table for HFE 4

CRD Node #	Critical Task #	CFM	Crew Failure Scenario #	HEP
3	1	AP-1: Key Alarm not Attended to	4	4.4E-03
		SA-4: Critical Data Dismissed/Discounted	16	0
4	2	AP-2: Misread or Skip Critical Step(s) in Procedure	7	1.0E-03
		SA-3: Critical Data Misperceived	11	1.6E-04
		E-2: Critical Data not Checked/Monitored with Appropriate Frequency	3	3.2E-02
4	3	E-3: Fail to Initiate Execution	5	1.4E-04
		E-4: Fail to Correctly Execute Response (Simple Task)	7	9.3E-06
Total HEP:				**3.8E-02**

*CFM AP-2 was identified as applicable for Critical Task 3 in the original analysis. The total HEP is adjusted for deleting the CFM from the applicable CFMs for the critical task.

As shown in the table above, the significant contributor to the HEP is Node 3. Workload is a dominating negative PIF. Workload is considered high for Node 3 because the general workload is considered higher than normal and there are many distractions when RCP B High Bearing Temperature Alarm occurs. However, workload for Node 4 is considered low because it is assumed that most of the crew will focus on AOP-018 and will not have additional distractions.

Table C-60 Workload Assessment Table for HFE 4

Task context	Assessment / Basis	Outcome (Extremely high/ moderately high/ nominal)	Comment
Scenario familiarity			
Multitasking	One operator has to respond to fire. The crew has to work in both Path-1 and APP-001-D1	Extremely high	
Distraction / interruption	Many alarms. Fire may distract the crew, but one operator is dedicated to response to fire	High	
Dynamics predictability	Many systems or components fail or become unavailable due to the electrical fault. It's difficulty for the crew to perform plant assessment.	High	
Time pressure			
Timing			
Hours in work			

C.5 Human Failure Event 5

C.5.1 PRA Scenario Description, Expected Operator Response and HFE Definition

This scenario is adapted from an actual event. See Scenario Descriptions for detailed information on sequence of key events.

Plant technical information:

- 3-loop Westinghouse pressurized water reactor (PWR)
- There are two main feedwater (FW) pumps: A and B
- There are three charging pumps: A, B and C
- There are three component cooling water (CCW) pumps: A, B and C

Situation from start:

- The plant is operating in Mode 1 at approximately 100% power.
- The Shift Manager and Shift Technical Advisor are outside of the control room at a shift turnover meeting.
- CCW Pump C and Charging Pumps A and C are running.
- FW Pumps A and B are running.

Event overview:

At 18:52, with the plant operating in Mode 1 at approximately 100% power, an electrical feeder cable failure caused an arc flash and fire on a non-vital electrical bus. The electrical bus failed to isolate due to a breaker failure, and the fault persisted much longer than design expectations. The effects were widespread throughout the electrical systems. The electrical isolations and automatic repowering also created time sequences that caused inadvertent equipment actuation and damage. The fault condition reduced voltage to Reactor Coolant Pump (RCP) B, causing an automatic reactor trip on Reactor Coolant System (RCS) loop low flow. Pressurizer level and pressure decreased due to RCS cooldown, resulting in an automatic safety injection (SI). Plant response was further complicated by multiple equipment malfunctions.

Loss of RCP seal injection and cooling:

Within the first minute of the initiating event, RCP seal cooling (via Component Cooling Water (CCW)) is lost due to the closing of Flow Control Valve (FCV) 626, the component cooling water thermal barrier outlet isolation valve. FCV-626 closed due to an inaccurate high-flow signal when the flow sensor lost power during electrical realignments resulting from the fault.

Approximately 27 minutes into the event, Chemical and Volume Control (CVC) Valve 310A fails open. When CVC-310A fails open the charging flow is diverted from the RCP seals to the RCS and RCP seal injection becomes inadequate (there is some injection flow, but it is inadequate to fulfill its safety function). As a result, the RCP seals begin to heat up and purge volume begins to empty.

Figure C-21~~Figure C-21~~ is the LOMFW event tree with the sequence highlighted.

Expected operator response:

With both RCP seal cooling from CCW unavailable and seal injection inadequate, the appropriate crew response would be to restore seal cooling from CCW to the RCP thermal barrier heat exchangers.

For successful recovery, operators would have to re-open FCV-626 from the control room before voiding within the RCPs occurs (see Figure C-22~~Figure C-22~~).

If FCV-626 is not opened in time or cannot be opened, operators would need to trip the running RCPs prior to failure of the seals. Figure C-23~~Figure C-23~~ is the LOSC event tree with the sequence highlighted.

If operators fail to stop the RCPs and restore cooling prior to the seals being fully challenged, the seals will fail at the maximum leakage rate of 480 gpm per RCP. The RCP seal failure will lead to a SLOCA. Pressurizer level will decrease, the pressurizer low pressure alarm will annunciate, and containment spray will activate with radiation alarms. The expected crew

response would be to initiate a cooldown and depressurization of the RCS to allow for the plant to be placed in shutdown cooling (SDC) using the residual heat removal (RHR) system. Figure C-24~~Figure C-24~~ is the SLOCA event tree with the sequence highlighted. Figure C-25~~Figure C-25~~ is the RCS cooldown fault tree.

HFE definition:

Failure to depressurize the RCS during a small loss of coolant accident (SLOCA).

To initiate a successful RCS cooldown, operators must depressurize the RCS by using the pressurizer PORVs or pressurizer sprays. The operators must also initiate a secondary side cooldown using the steam generator atmospheric relief valves or the turbine bypass valves to remove the decay heat and depressurize the RCS.

Operators would have at least two hours to initiate the RCS cooldown and depressurization prior to depletion of the RWST inventory during an SLOCA caused by failure of RCP seals.

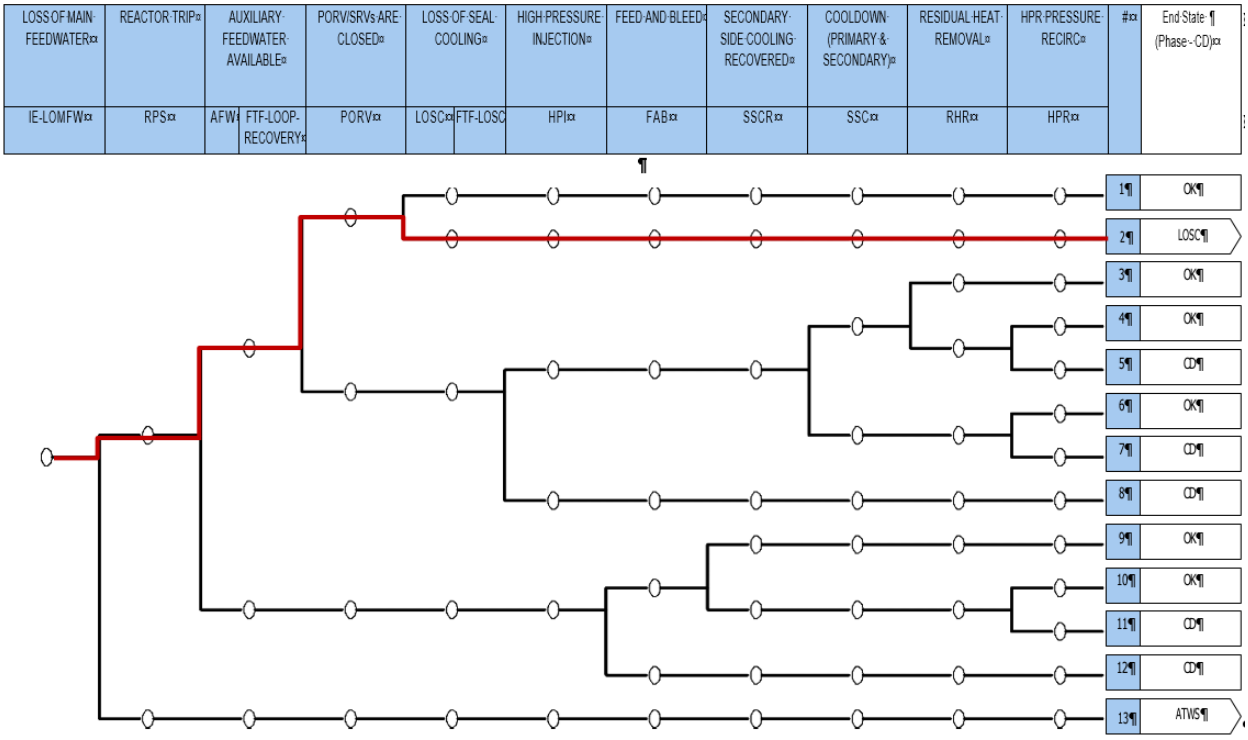


Figure C-21 Loss of Main Feedwater Event Tree for HFE 5

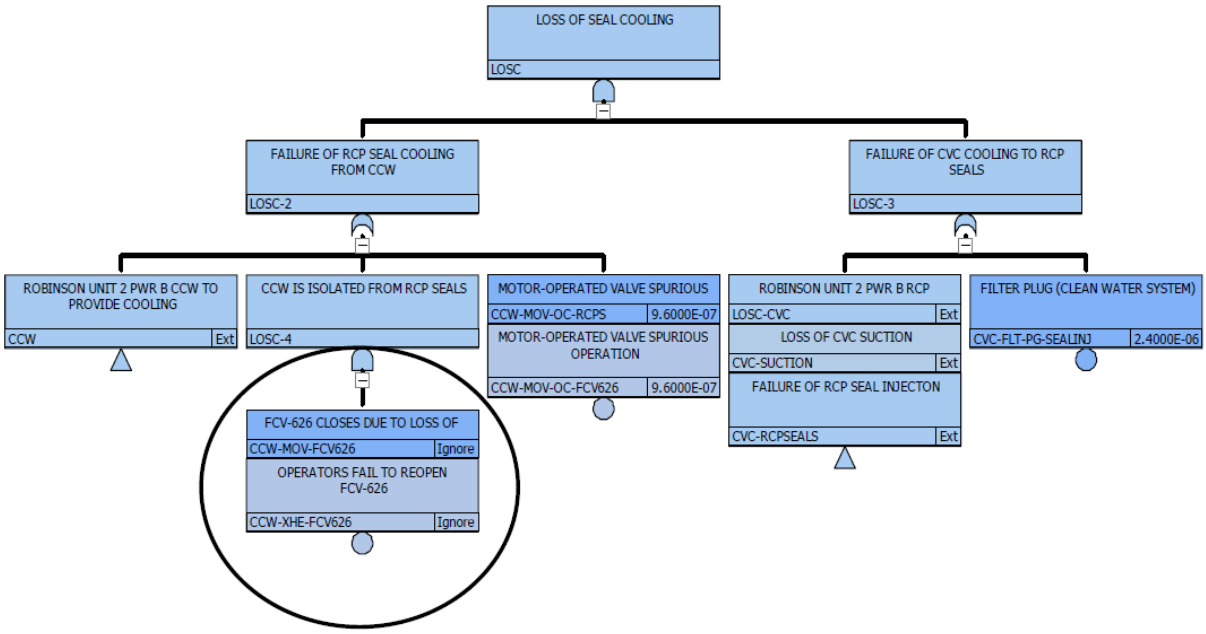


Figure C-22 Loss of Seal Cooling Fault Tree for HFE 5

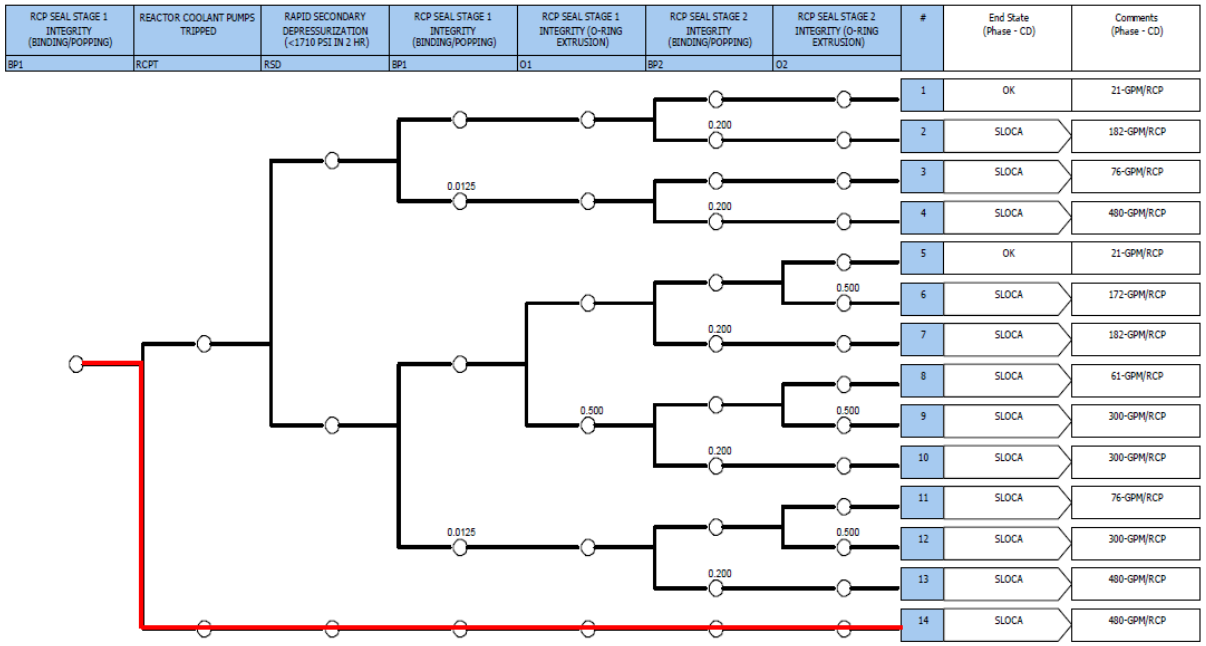


Figure C-23 Loss of Seal Cooling Event Tree for HFE 5

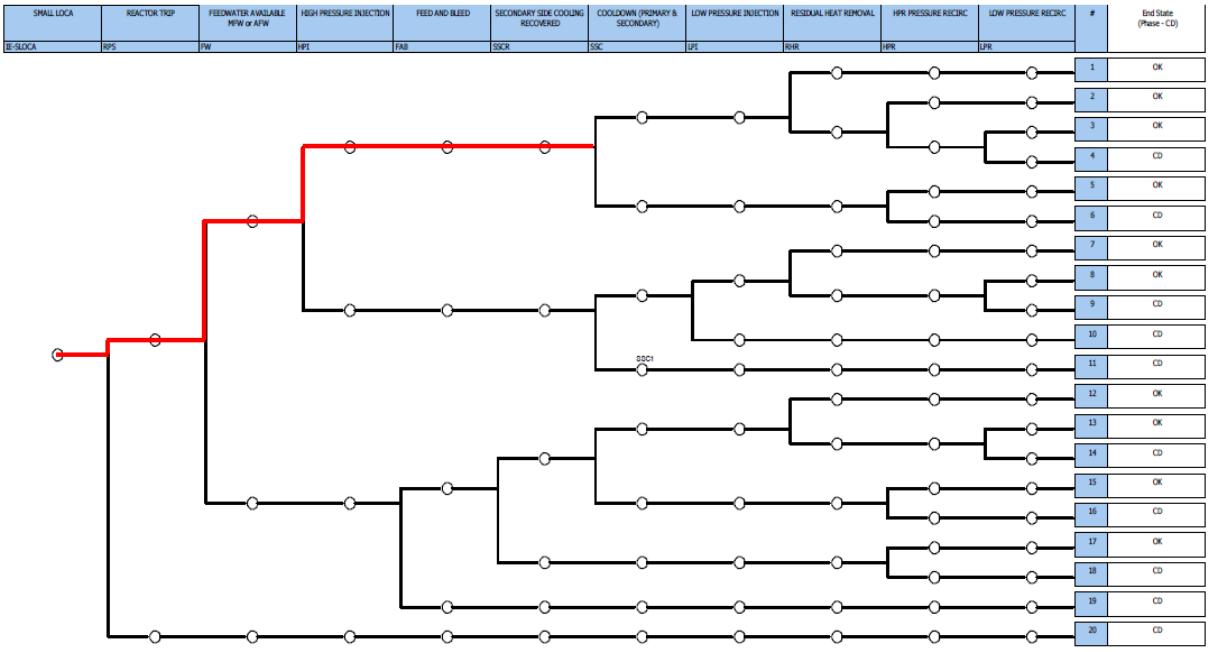


Figure C-24 Small Loss of Coolant Accident Event Tree for HFE 5

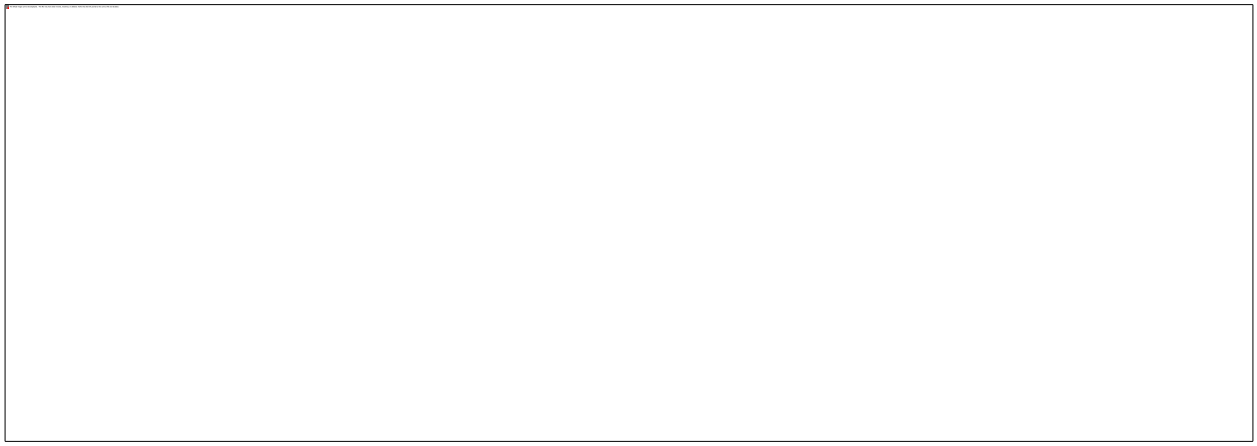


Figure C-25 RCS Cooldown Fault Tree for HFE 5

C.5.2 Crew Response Diagram and Task Analysis

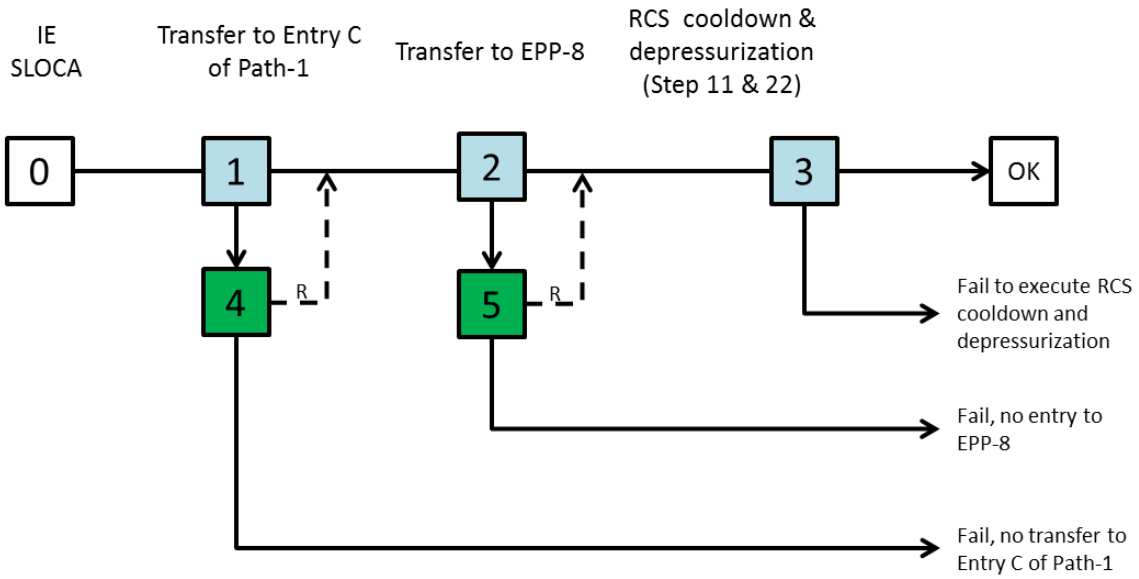


Figure C-26 Crew Response Diagram for HFE 5

C.5.2.1 Node 0: Initiating event (SLOCA)

Node 0 represents the initiating event – SLOCA. According to information from HFE-4, RCP will fail 19 minutes after seal cooling and injection is lost. Based on the information from the operator interview, the SLOCA will occur at 19:38. It is assumed that

- Seals of all 3 RCPs have failed.
- The RCS temperature is at 540°F and cools down at ½ °F/min (30°F/hour) once the SLOCA begins due to hot water being lost out the seals and cold water being injected by the SI pumps.
- The crew is at the diamond at B15 reading "PZR SPRAY AND AUX SPRAY VALVES CLOSED" when SLOCA occurs.

C.5.2.2 Node 1: Transfer to Entry C of Path-1

Within 30 seconds of SLOCA, alarms B-2, C-2, D-2, and F-2 will cascade in. At this point, distractions die down and the BOP is reintegrated to the rest of the crew after dedicated to the fire procedure (AOP-041) for 40 minutes (i.e., 18:52 through 19:32). Thus, it is expected that the crew will detect these alarms and one operator will enter AOP-018 Section C to trip the RCPs. The operator will not be in AOP-018 long before he/she exits the procedure. Note that it is estimated in HFE 4 that it takes 3 minutes to trip the RCPs from the entry of AOP-018 Section C.

Between 19:42 and 19:46, the crew will receive the following cues:

- High CV pressure

- High sump level
- Pressurizer low pressure alarm
- Decreasing pressurizer level
- Abnormal radiation

The cue pattern, decreasing workload, increasing manpower, and training may help the crew recognize SLOCA, but they will continue in Path-1 to find a way to transfer to EPP-8 (Post LOCA Cooldown and Depressurization).

Entry of EPP-8 would require a transfer to Entry C of Path-1 at one of the following diamond steps at B4 and B5 of Path-1 (see Figure C-27~~Figure C-27~~):

- R-2, R-32A, R-32B RAD LEVELS NORMAL
- CV PRESS NORMAL
- CV SUMP LEVEL NORMAL

The diamond step “CV PRESS NORMAL” could be reached within 3 minutes from B15 if no other procedures are performed in parallel. Since one operator will enter AOP-018 after the SLOCA, it is estimated that the crew will reach the step within 5 minutes (i.e., 19:43). The vapor pressure in the containment will be elevated enough in 3 minutes (i.e., 19:41) after the SLOCA for the gauges to definitely indicate abnormal readings. Hence, when the crew reach the diamond step “CV PRESS NORMAL”, the condition of transferring to Entry C has been met. Considering the RAD abnormal level alarms will be annunciated at around 19:46, the diamond step “CV PRESS NORMAL” is the first opportunity to transfer to Entry C.

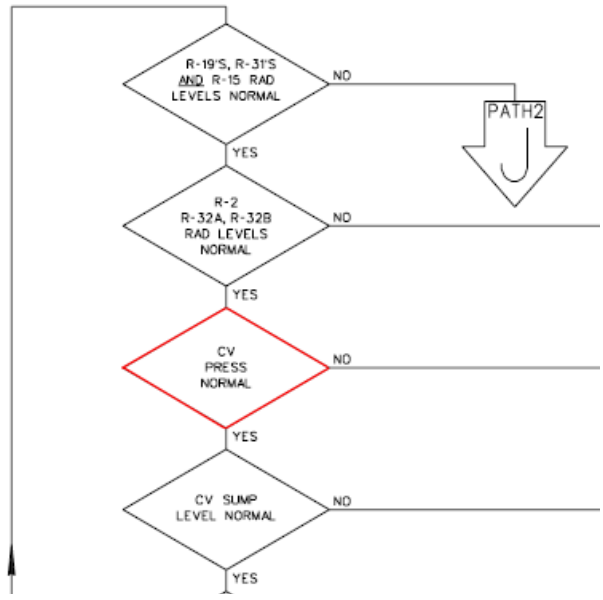


Figure C-27 Step in Path-1 to Check CV Pressure for HFE 5

The critical tasks associated with Node 1 include:

- Check CV pressure and transfer to Entry C of Path-1

C.5.2.3 Node 2: Transfer to EPP-8

At J13, the crew will be asked to check if RCS pressure is greater than 275 PSIG, which it will be in this case. Next, the crew will be asked to obtain RCS boron, activity, and H2 samples and then enter EPP-8 (see Figure C-28~~Figure C-28~~).

It will take between 12 and 42 minutes to reach J13 from B15. Considering that the distractions have died down and the BOP operator has reintegrated with the crew, it is assumed that the crew will reach J13 in 27 minutes (i.e., average of 12 and 42) from B15 (i.e., 20:05). Given the cooldown rate of ½ °F/min, the RCS temperature at the transfer is about 526 °F.

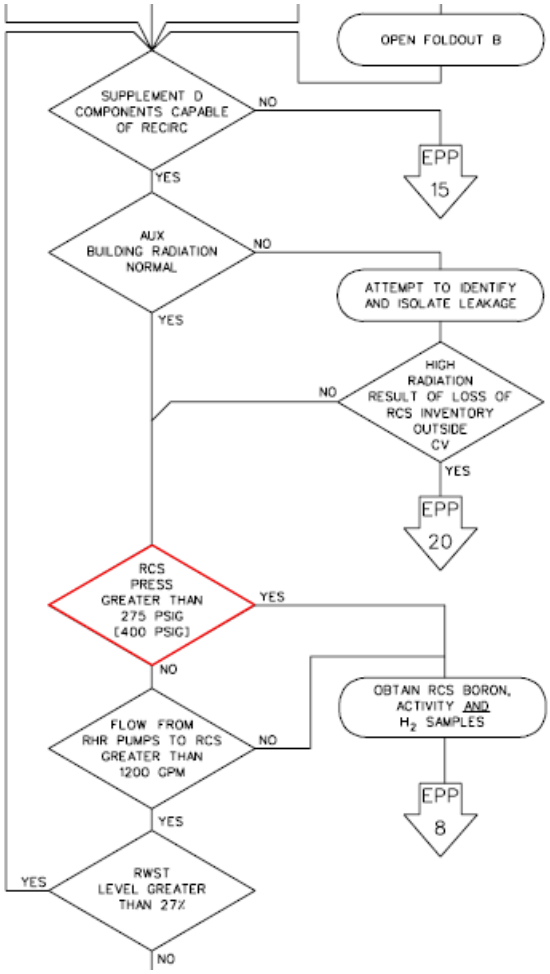


Figure C-28 Step in Path-1 to Check RCS Pressure for HFE 5

The critical tasks associated with Node 2 include:

- Check RCS pressure and transfer to EPP-8

C.5.2.4 Node 3: RCS cooldown and depressurization

After entry of EPP-8, the crew will open Foldout B and then proceed through the steps of the procedure, stopping RHR pumps when RCS pressure is greater than 275 psig, which it will be in

this case, checking emergency busses and non-emergency AC busses, establishing charging flow, and controlling SG levels. The crew will be asked to start cooldown at Step 11 and depressurization at Step 22 as quickly as possible (see note above Step 11). It will take about 6 minutes to reach Step 11 after entry of EPP-8. Given the cooldown rate of ½ °F/min, the RCS temperature is about 523 °F when the crew reaches Step 11.

At Step 11, the crew will start cooldown at the maximum rate of 100°F/hr. It takes 74 minutes to get the plant cooled down below 400 °F (i.e., 21:25), which is within the 2-hour time window. That is, the crew is on track to get SDC in service (i.e., complete step 50) prior to running out of RWST inventory.

Uncertainty analysis:

> If it takes 42 minutes (i.e., upper bound of the time estimate) to reach J13 from B15 (i.e., 20:20), the RCS temperature will be about 519 °F at entry of EPP-8, and 516 °F at Step 11 of EPP-8. With a maximum cooldown rate of 100°F/hr, it will take about another 70 minutes to get the plant cooled down below 400 °F (i.e., 21:36), which is also within the 2-hour time window.

The performance of the cooldown and depressurization is a prolonged control action with continuous potential for mid-course corrections (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. Thus, Steps 11 through 22 are modeled as one node for execution without recovery.

Step 11 is listed in Figure C-29~~Figure C-29~~ and step 22 is listed in Figure C-30~~Figure C-30~~.

The critical tasks associated with Node 3 include:

- Cooldown and depressurize the RCS per procedural directions

NOTE

- A differential pressure of 210 psid across the RCP number 1 seals is necessary for continued RCP operation.
- RCS cooldown should be completed as quickly as possible since the RCS may continue to depressurize to a value that may not support differential pressure across the RCP number 1 seals.

11. Initiate RCS Cooldown To Cold Shutdown As Follows:

a. Maintain cooldown rate in RCS cold legs less than 100°F/hr in the last 60 minute	
b. Maintain RCS temperature and pressure within limits of curve 3.4, reactor coolant system pressure - temperature limitations for cooldown	
c. Check steam dump to Condenser - AVAILABLE	c. Dump steam from intact S/Gs using STEAM LINE PORVs. Go To Step 12.
d. Dump steam to Condenser from intact S/Gs	

Figure C-29 Step 11 in Procedure for HFE 5

*22. Depressurize RCS To Refill PZR As Follows:

a. Check PZR level - LESS THAN 24% [45%]	a. Go To Step 23.
b. Use normal PZR Spray to depressurize the RCS	b. Use one PZR PORV. IF no PZR PORV is available, THEN use Auxiliary Spray.
c. Check PZR level - GREATER THAN 24% [45%]	c. WHEN PZR level greater than 24% [45%], THEN stop RCS depressurization. Go To Step 23.
d. Stop RCS depressurization	

Figure C-30 Step 22 in Procedure for HFE 5

C.5.2.5 Node 4: Recovery of Node 1

Based on the operator interview, the CV sump level abnormal alarm will be annunciated between 19:42 and 19:46. Thus, if the crew does not transfer to Entry C at the diamond step "CV PRESSURE NORMAL" at E5, the diamond step "CV SUMP LEVEL NORMAL" can serve as a recovery opportunity.

If the crew misses both steps, they will back to B12 and then transfer to Entry C at the diamond step "R-2, R-32A, R-32B RAD LEVELS NORMAL" at E4. It is estimated that this recovery opportunity will take extra 15 minutes. That is, it will the crew 42 minutes (i.e., 27 + 15) to reach J13 from B15. Based on the uncertainty analysis in Node 3, this recovery opportunity is also feasible assuming the crew reaches J13 in 27 minutes after SLOCA. If it takes more than 27 minutes, this recovery is infeasible.

C.5.2.6 Node 5: Recovery of Node 2

The diamond step "FLOW FROM RHR PUMPS TO RCS GREATER THAN 1200 GPM" serves as a recovery opportunity if the crew does not transfer to EPP-8 from the diamond step "RCS PRESS GREATER THAN 275 PSIG". In addition, the RWST level is expected to be greater than 27% since this is a small LOCA. Thus, when the crew reaches the diamond step "RWST LEVEL GREATER THAN 27%", they will take the YES branch, which will provide another opportunity to check RCS pressure (see Figure C-28~~Figure C-28~~). However, if it takes 15 minutes to recover the error in Node 3 (see discussion on Node 4), this recovery opportunity may not be feasible given the 2-hour time window.

C.5.2.7 Task Analysis

Table C-61 Task Analysis for HFE 5

CRD Node #	Critical Task #	Critical Task Description	Required Activities	Additional Information
1	1	Check CV pressure and transfer to Entry C of Path-1	• Identify correct data source • Interpret plant parameter correctly (comparing against preset numerical criteria) • Make procedure transfer	The criteria are numerical, requiring no additional judgment.
2	2	Check RCS pressure and transfer to EPP-8	• Identify correct data source • Interpret plant parameter correctly (comparing against numerical criteria in procedure) • Make procedure transfer	The criteria are numerical, requiring no additional judgment.
3	3	Cooldown and depressurize the RCS	Modeled as a complex action. There is no need to document various associated activities. The CFM for failure to execute a complex procedure does not distinguish between the various activities.	

C.5.3 Timeline

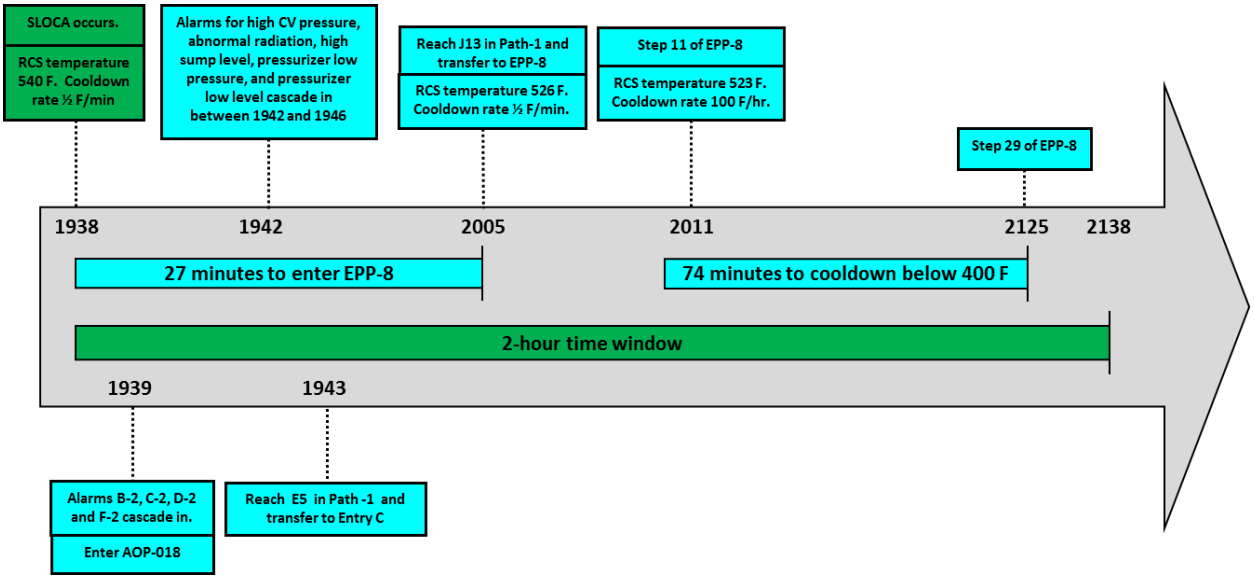


Figure C-31 Timeline for HFE 5

The following information was obtained through discussion with plant staff.

- SLOCA occurs at 19:38, 19 minutes after CVC-310A opens
- Alarms B-2, C-2, D-2, and F-2 will occur within 1 minute after SLOCA.
- It takes 5 minutes to reach the diamond step “CV PRESS NORMAL” at E5 in Path-1.
- It takes 27 minutes to reach J13 from B15.
- It takes about 6 minutes to reach Step 11 after entry of EPP-8.

C.5.4 Evaluation of Crew Failure Modes (CFMs) and Decision Trees

C.5.4.1 Critical Task 1

Table C-62 CFM Selection Table for HFE 5, Critical Task 1

CRD Node	1		
Critical Task	1		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	Directed search by procedure	
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable but unlikely	8
SA-1: Data Misleading or Not Available	No	Instrumentation works properly and indications are available in the MCR.	

SA-2: Wrong Data Source Attended To	Yes	Applicable but unlikely.	12
SA-3: Critical Data Misperceived	Yes	Potentially applicable	12
SA-4: Critical Data Dismissed/Discounted	No	No valid alternative scenario	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	No	Simple transfer with no further decision required.	
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	No	Not an execution step	
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
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	Not an execution step	

Table C-63 Evaluation of CFM AP-2 for HFE 5, Critical Task 1

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	**Assessment**	**Justification**
Workload	High	One operator is in AOP-018 tripping RCPs. Many alarms associated with SLOCA.
Procedure	Simple	Procedure is straightforward.
Compensatory Factors	Present	Assuming nominal operation practice.
Recovery Potential	Yes	
Crew Failure Scenario #		*8*

Table C-64 Evaluation of CFM SA-2 for HFE 5, Critical Task 1

SA-2: Wrong Data Source Attended to		
PIF	**Assessment**	**Justification**
HSI	Good	Assuming nominal HSI
Workload	High	One operator is in AOP-018 tripping RCPs. Many alarms associated with SLOCA.
Familiarity with Data Source	Good	
Recovery Potential	Yes	
Crew Failure Scenario #		*12*

Table C-65 Evaluation of CFM SA-3 for HFE 5, Critical Task 1

SA-3: Critical Data Misperceived		
PIF	**Assessment**	**Justification**
HSI/Environment	*Good*	Assuming nominal HSI
Workload	*High*	One operator is in AOP-018 tripping RCPs. Many alarms associated with SLOCA.
Training	*Good*	The crew performs some type of LOCA scenario 4 to 5 times per year and at least one of these is a seal LOCA.
Recovery Potential	*Yes*	
Crew Failure Scenario #		*12*

C.5.4.2 Critical Task 2

Table C-66 CFM Selection Table for HFE 5, Critical Task 2

CRD Node	2		
Critical Task	2		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	Directed search by procedure	
AP-2: Misread or Skip Critical Step(s) in Procedure	Yes	Applicable but unlikely	14
SA-1: Data Misleading or Not Available	No	Instrumentation works properly and indications are available in the MCR.	
SA-2: Wrong Data Source Attended To	Yes	Applicable but unlikely.	16
SA-3: Critical Data Misperceived	Yes	Potentially applicable.	16
SA-4: Critical Data Dismissed/Discounted	No	No valid alternative scenario	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	No	Simple transfer with no further decision required.	
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	No	Not an execution step	
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
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	Not an execution step	

Table C-67 Evaluation of CFM AP-2 for HFE 5, Critical Task 2

AP-2: Misread or Skip Critical Step(s) in Procedure		
PIF	**Assessment**	**Justification**
Workload	Low	The distraction has died down and the crew focuses on Path-1.
Procedure	Simple	Procedure is straightforward.
Compensatory Factors	N/A	
Recovery Potential	Yes	
Crew Failure Scenario #		*14*

Table C-68 Evaluation of CFM SA-2 for HFE 5, Critical Task 2

SA-2: Wrong Data Source Attended to		
PIF	**Assessment**	**Justification**
HSI	Good	Assuming nominal HSI
Workload	Low	The distraction has died down and the crew focuses on Path-1.
Familiarity with Data Source	Good	The crew performs some type of LOCA scenario 4 to 5 times per year and at least one of these is a seal LOCA.
Recovery Potential	Yes	
Crew Failure Scenario #		*16*

Table C-69 Evaluation of CFM SA-3 for HFE 5, Critical Task 2

SA-3: Critical Data Misperceived		
PIF	**Assessment**	**Justification**
HSI/Environment	*Good*	Assuming nominal HSI
Workload	*Low*	The distraction has died down and the crew focuses on Path-1.
Training	*Good*	The crew performs some type of LOCA scenario 4 to 5 times per year and at least one of these is a seal LOCA.
Recovery Potential	*Yes*	
Crew Failure Scenario #		*16*

C.5.4.3 Critical Task 3

Table C-70 CFM Selection Table for HFE 5, Critical Task 3

CRD Node	3		
Critical Task	3		
CFMs	**Applicable? (Yes/No)**	**Justification**	**Scenario #**
AP-1: Key Alarm not Attended to	No	No alarm	
AP-2: Misread or Skip Critical Step(s) in Procedure*	No	N/A. Execution step.	
SA-1: Data Misleading or Not Available	No	N/A. Execution step.	
SA-2: Wrong Data Source Attended To	No	N/A. Execution step.	
SA-3: Critical Data Misperceived	No	N/A. Execution step.	
SA-4: Critical Data Dismissed/Discounted	No	N/A. Execution step.	
SA-5: Premature Termination of Critical Data Collection	No	The CFM is irrelevant because the operators are not monitoring a plant parameter.	
RP-1: Misinterpret Procedures	No	Procedure is clear.	
RP-2: Choose Inappropriate Strategy	No	No other strategy in procedure.	
E-1: Delay Implementation	No	No apparent complicating factors to delay implementation. Only action in the queue.	
E-2: Critical Data Not Checked/Monitored with Appropriate Frequency	No	The operators are not monitoring a plant parameter.	
E-3: Fail to Initiate Execution	Yes	Applicable but unlikely. Procedural direction is to trip RCPs, which is the only action in the queue.	5
E-4: Fail to Correctly Execute Response (Simple Task)	No	Complex task	
E-5: Fail to Correctly Execute Response (Complex Task)	Yes	Control actions	7

Table C-71 Evaluation of CFM E-3 for HFE 5, Critical Task 3

E-3: Fail to Initiate Execution		
PIF	**Assessment**	**Justification**
Immediacy	Yes	The crew is aware of SLOCA. Thus, they will not hesitate to start RCS cooldown or depressurization, which is the only action in the queue. The note above Step 11 tells the crew to perform the action as quickly as possible.
Workload	N/A	
Recovery Potential	N/A	
Crew Failure Scenario #		*5*

Table C-72 Evaluation of CFM E-5 for HFE 5, Critical Task 3

E-5: Fail to Correctly Execute Response (Complex Task)		
PIF	**Assessment**	**Justification**
Execution Straightforward	*No*	Control actions are, by definition, not straightforward.
Training	*Good*	
Work Practices	*Good*	Procedure contains verification actions.
Recovery Potential	*No*	There is no recovery potential for control actions.
Crew Failure Scenario #		*7*

C.5.5 Summary of Analysis

Shortly after the SLOCA, the crew will be busy with the alarms and entering AOP-018 to trip RCPs. After they exit AOP-018 and focus on Steps in Path-1, the workload will become normal as the distractions dies down. Other conditions are nominal.

Although the crew may recognize SLOCA based on the cue pattern, they will have to continue in Path-1 to find a transfer point to transition to EPP-8, which requires a transfer to Entry C.

After the crew enters EPP-8, Steps 11 and 22 ask the crew to start RCS cooldown and depressurization as quickly as possible. There is no real diagnosis or kick-outs before Step 11.

Based on the operator interview, it will take 12 – 42 minutes to reach J13 from B15. As discussed in Node 3, the upper bound allows the crew to get the plant cooled down below 400 °F within 2 hours.

<u>Recovery analysis:</u>

At Node 1 and Node 2, if the crew misses the first procedure transfer opportunity, other procedure transfer opportunities serve as recovery. However, the 2-hour time window does not give much margin for recovery. As discussed in Node 4 and Node 5, if the crew misses the first

recovery opportunity in Node 1 or Node 2 or it takes the crew more than 27 minutes to make it to J13 from B15, the second recovery opportunities may become infeasible.

Table C-73 HEP Calculation Table for HFE 5

CRD Node #	Critical Task #	CFM	Crew Failure Scenario #	HEP
1	1	AP-2: Misread or Skip Critical Step(s) in Procedure	8	1.5E-04
		SA-2: Wrong Data Source Attended to	12	3.2E-04
		SA-3: Critical Data Misperceived	12	3.4E-05
2	2	AP-2: Misread or Skip Critical Step(s) in Procedure	14	1.2E-04
		SA-2: Wrong Data Source Attended to	16	5.2E-05
		SA-3: Critical Data Misperceived	16	1.3E-05
3	3	E-3: Fail to Initiate Execution	5	1.4E-04
		E-5: Fail to Correctly Execute Response (Complex Task)	7	3.8E-03
Total HEP:				**4.6E-03**

* CFM AP-2 was identified as applicable for Critical Task 3 in the original analysis. The analysis was corrected because CFM AP-2 is not applicable for execution tasks.

As shown in the table above, high workload and complex execution are two main drivers of the HEP.

APPENDIX D
PROPOSED ANALYSIS APPROACH FOR HUMAN FAILURE EVENTS 3 AND 4

D.1 Introduction

The application of the IDHEAS AT-POWER method relies on the analysts being able to identify a procedural path that would lead to success. The crew failure modes (CFMs) defined in the method are based on the generic cognitive tasks in crew responses performed when following operating procedures. One of the assumptions of the method was that the operating procedures are unambiguous and valid for the challenges being addressed. As discussed in Section 4.6.3, this was not the case for the responses associated with Human Failure Events 3 and 4. While there were several steps in the procedures that would have led to reestablishing cooling to the reactor coolant pump (RCP) seals by opening the flow control valve FCV-626, or tripping the reactor coolant pumps when necessary, there was no single, unambiguous path to these steps. As discussed in Section 3 of this appendix, choosing a particular path would involve the crew making decisions based on resources, or drawing conclusions based on an understanding of the intent of a procedural step rather than on a literal reading of the procedure. The crew failure modes defined for IDHEAS AT-POWER do not address these types of decisions. Faced with this situation, the analyst teams made assumptions about the crews' behavior to establish a representative path with which to analyze Human Failure Events 3 and 4. However, recognizing that the choice of path is uncertain, a more comprehensive approach would entail considering the different success paths. The paths would differ according to the decisions or choices made by the crew at various points while following the procedures. For each success path the conditional human error probability (HEP) would be developed using the crew failure modes and decision trees of IDHEAS AT-POWER. The total human error probability would be evaluated by a probabilistic weighting of the conditional human error probabilities for each path, with the weights representing the likelihood of following the particular procedural success path.

The scenario being assessed, the probabilistic risk assessment (PRA) model used to analyze the scenario, and the two human failure events are defined in Appendix A-2 and will not be repeated here. Section 2 provides an analysis of the procedural paths that would lead to success in either restoration of cooling or, if necessary, tripping the reactor coolant pumps. As will become evident, the two responses, opening FCV-626 and tripping the reactor coolant pumps, while performing different functions, are highly dependent since, as illustrated in Figure D-1~~Figure D-1~~, the procedural paths are intertwined. Success in the first response prevents the seal loss of coolant accident from occurring; the second lessens the likelihood of the seal loss of coolant accident becoming equivalent to a small loss of coolant accident. Success in restoring cooling precludes the need to trip the reactor coolant pumps. However, on some paths, success in tripping the reactor coolant pumps is achieved at the expense of reestablishing cooling. Section 3 provides an overview of how the human error probabilities would be evaluated using this approach. This is an extension of the IDHEAS AT-POWER method and is presented here as one possible approach to dealing with ambiguous or incomplete operating procedures, where the type of decisionmaking required by the operators is not addressed by the existing crew failure modes. Section 4 provides some concluding remarks.

D.2 Scenario Map and Identification of Success Paths

Figure D-1~~Figure D-1~~ provides a scenario map indicating paths for success in either opening the FCV-626 or tripping the reactor coolant pumps should that become necessary. The starting point is the assumption that the crew reenters Path-1 at 19:00 upon automatic SI due to a rapid cooldown. There are two procedural steps providing guidance for the crew to open FCV-626:

- Step 4.2 of APP-001-D1 (Annunciator Panel Procedure)
- Step 10 of Section C of AOP-018 (Reactor Coolant Pump Abnormal Conditions)

In addition, the following two procedure steps provide guidance for the crew to trip the reactor coolant pumps:

- Path-1 C11
- Step 3 of Section C of AOP-018 (Reactor Coolant Pump Abnormal Conditions)

As illustrated in Figure D-1~~Figure D-1~~, there are four procedural paths leading to AOP-018 and one path to APP-001-D1. Following some procedural paths will make one or both responses infeasible. Which procedural path the crew takes is determined by their decisions at the four decision points represented by the diamonds in the figure. In the following sub-sections, the uncertainty associated with the decision points and their impact on the procedural paths and success or failure of the responses is discussed.

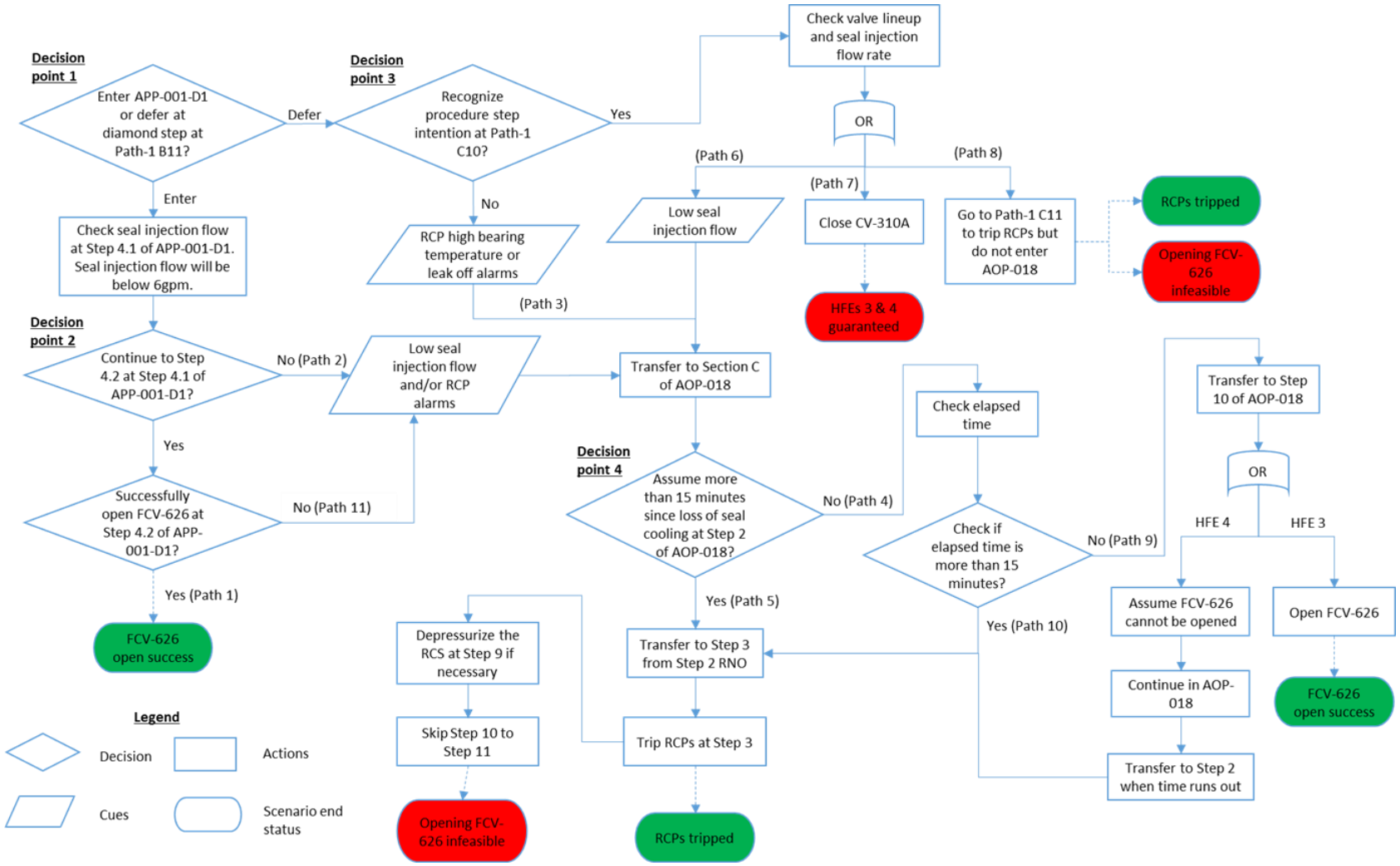


Figure D-1 Scenario Map for HFE 3 and HFE 4

D.2.1 Decision Point 1: Enter APP-001-D1 or defer at diamond step at Path-1 B11

The diamond step at Path-1 B11 will direct the crew to check the reactor coolant pump thermal barrier cooling water low flow annunciator (see the highlighted diamond step in Figure D-2~~Figure D-2~~). This provides an opportunity to recognize loss of seal cooling (LOSC) from component cooling water (CCW) due to the closure of FCV-626.

According to the scenario description, this annunciator is annunciated when FCV-626 closes at 18:52. However, many systems and components fail or become unavailable due to the electrical fault. Workload is expected to be extremely high at the beginning of the scenario – the crew is busy with the reactor trip, safety injection (SI), and responding to the fire at the same time, especially when the balance of plant (BOP) operator is dedicated to AOP-041, Response to Fire Event, for about 40 minutes. Therefore, the crew could either fail to notice the reactor coolant pump thermal barrier cooling water low flow annunciator or choose not to respond to it. The rationale for not responding to the alarm would be that restoring seal cooling from component cooling water is not a priority at the beginning of the scenario, given that the crew has started Charging Pumps B and C per Path-1 to restore reactor coolant pump seal injection at 18:53. Even when safety injection is automatically actuated at 19:00, Charging Pump B is still running, and should provide adequate seal injection.

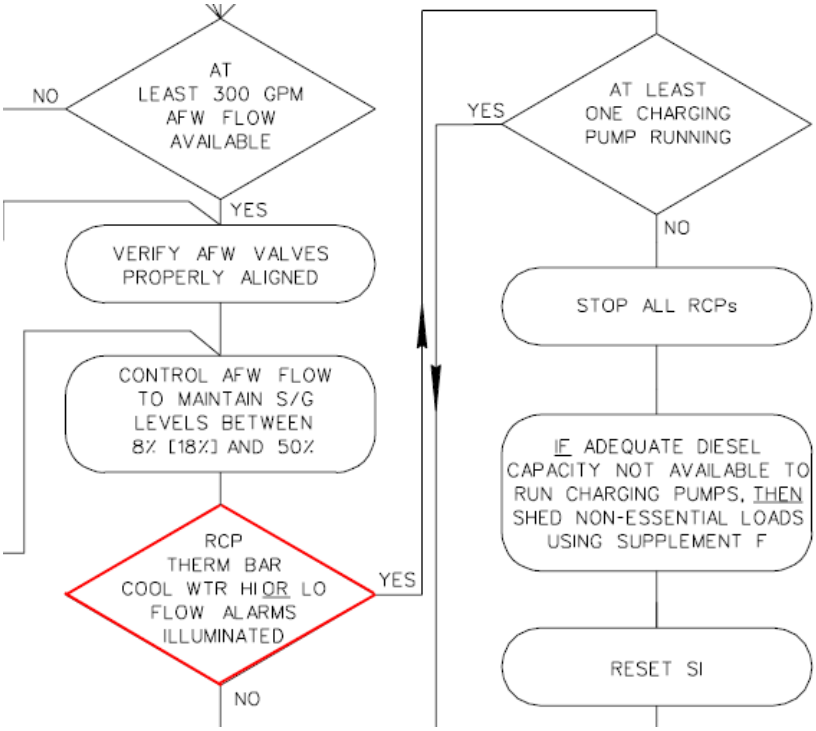


Figure D-2 Procedural step in Path-1 to Check the Reactor Coolant Pump Thermal Barrier Cooling Water Low Flow Annunciator

However, seal injection becomes inadequate when chemical volume control valve CVC-310A fails fully open at 19:19. The crew will reach the diamond step at Path-1 B 11 about 30 minutes after the reactor trip (i.e., 19:22). As such, when the crew reaches the step, seal injection will have become inadequate, although it may not be evident to the crew at this time.

Based on discussion with plant staff, whether the crew will enter APP-001-D1 largely depends on whether the crew has enough manpower, given that, as discussed above, the crew may still think that restoring seal cooling from component cooling water is not their priority. At this point, the plant has come to a relatively more stable state compared to the beginning of the scenario as distractions die down. Although the balance of plant operator is still dedicated to AOP-041 and workload is still considered higher than normal, workload becomes relatively lower. However, it is uncertain whether the workload level is sufficiently low so that the crew will definitely enter APP-001-D1.

- If the crew chooses to enter APP-001-D1, they will proceed to Step 4.1 (see discussion in Section 2.2).
- If the crew chooses to defer entry of APP-001-D1, they will continue in Path-1 to the diamond step at C10 (see discussion in Section 2.3).

D.2.2 Decision Point 2: Continue to Step 4.2 at Step 4.1 of APP-001-D1

Step 4 of APP-001-D1 is listed below.

Step 4:

IF FCV-626 has failed closed, THEN PERFORM the following:

4) VERIFY RCP Seal Injection flow 6gpm to 20 gpm.
5) ATTEMPT to reopen FCV-626
6) IF FCV-626 will NOT reopen, THEN INITIATE action to restore FCV-626 to OPERABLE status and CONTACT Engineering for assistance.

At this point, CVC-310A has failed fully open and seal injection is below 6gpm, which is considered inadequate. This is a cue for the crew to realize loss of seal injection. Since the procedure does not indicate what to do if the flow rate is less than 6gpm, the crew can choose to:

- Continue to Step 4.2 to open FCV-626, which provides a success path for restoration of cooling (Path 1).

OR

- Enter Section C of AOP-018 (Reactor Coolant Pump Abnormal Conditions) without going to Step 4.2 based on training on diagnosis of loss of seal injection (Path 2).

OR

- Enter Section C of AOP-018 (Reactor Coolant Pump Abnormal Conditions) after they attempt but fail to open FCV-626 based on training on diagnosis of loss of seal injection (Path 11). It the crew were to enter APP-001-D1 they would do so at around 19:22 and reach Step 4.2 around 19:24, when reactor coolant pump B High Bearing Temperature Alarm will be annunciated. If the crew cannot open FCV-626, this alarm and other following reactor coolant pump alarms will reinforce their decision to transfer to Section C of AOP-018, given that they are already aware that the seal injection flow is insufficient.

D.2.3 Decision Point 3: Recognize procedure step intention at Path-1 C10

As discussed in Section 2.1, if the crew defers entry of APP-001-D1, they would continue to the diamond step at C10 (see Figure D-3~~Figure D-3~~). Taken literally, the intent of this step is to check if there is sufficient seal injection by checking that at least one charging pump is running.

- If the crew understands the intent of this step (i.e., to establish that there is sufficient seal injection), they could check the valve lineup and seal injection flow rate, which will be below 6gpm. This would be a cue for the crew to recognize loss of seal injection. At this point, the crew could:
    - Enter Section C of AOP-018 based on the low seal injection flow rate (Path 6).

OR

    - Actively investigate the cause of loss of seal injection, identify failure of CVC-310A, and then try to close the valve to restore seal injection. In this case, we have assumed that this would take too much time and both responses would become infeasible (Path 7).

OR

    - Go to the next step in Path-1 to stop all RCPs when they discover that all seal cooling is lost (Path 8).

- If the crew takes the step at face value, they will conclude that there is sufficient seal injection and continue in Path-1, bypassing the step to trip RCPs in Path-1. In this case, it is assumed that the crew will transfer to Section C of AOP-018 when they receive RCP high bearing temperature or leak-off alarms (Path 3).

Note that Crew Failure Mode SA1 “Data Misleading” could apply to this procedural step. However, this crew failure mode is not a direct contributor to either Human Failure Event 3 or 4. As discussed above, how the crew responds to this step takes the crew down different paths. Nevertheless, the decision tree for this crew failure mode could be used to assess the probability of following path 3 rather than one of paths 6, 7, or 8. However, the relative likelihoods of following paths 6, 7, and 8 are not addressed by the current crew failure modes. On further discussion with plant staff one or more of these paths could be eliminated.

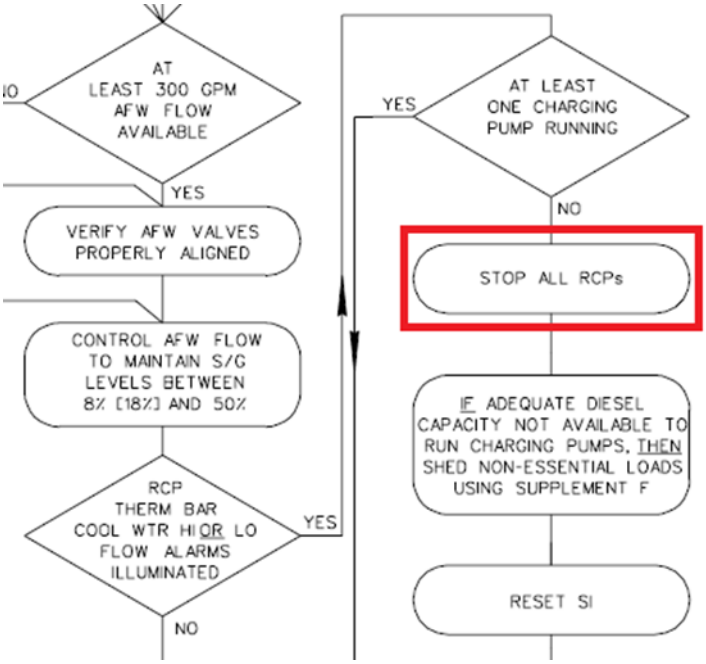


Figure D-3 Step in Path-1 to trip RCPs

D.2.4 Decision Point 4: Has it been more than 15 minutes since loss of seal cooling (Step 2 of AOP-018)?

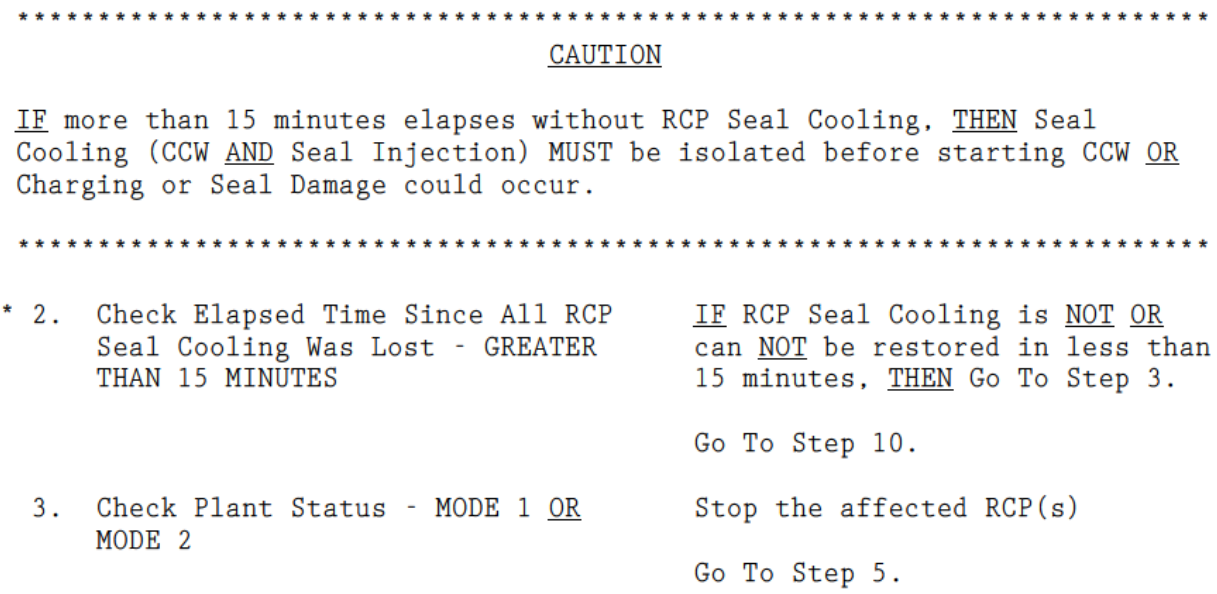
Step 2 and its response not obtained (RNO) column of Section C of AOP-018 is shown in Figure D-4~~Figure D-4~~.

At Step 2, the crew will need to determine how long seal injection has been lost. Since the loss of seal injection from the charging pumps was gradual, it would be difficult for the crew to determine the time when seal injection has been lost. Furthermore, there is no crew failure mode for this type of forensic, backward-looking assessment. There are several possibilities for modeling this.

- The crew may assume that more than 15 minutes has elapsed, particularly considering they may not have enough manpower to do this task. In this case, the crew would go to Step 3 from the Step 2 RNO column to stop all reactor coolant pumps (Path 5). Then, they will depressurize the reactor coolant system if necessary to less than 1700psig at Step 9. Next, the crew will skip Step 10 to Step 11, thus bypassing the instruction to open FCV-626. Although this path would give the crew an opportunity to do seal injection beyond Step 10, this was not identified as a success path for this PRA model. Note that, in fact, Step 5 of AOP-018 directs the crew to close FCV-626.
- The crew may choose to check how long seal injection has been lost rather than to make an assumption. In this case, their next actions would depend on the results of their assessment (which would depend on which procedural path they took to Step 2 of AOP-018 and how fast they moved through procedures). Take Path 2 for example, the crew is expected to enter APP-001-D1 around 19:22. It will take them about 1 minute to check RCP seal injection flow rate, 2 minutes to transfer to Section C of AOP-018 from APP-001-D1 (19:25), and 1 minute to reach Step 2 (19:26). That is, 7 minutes will have elapsed since valve CVC-310A failed fully open. If the crew takes other procedural paths or moves more slowly

through procedures, it is possible that 15 minutes will have elapsed when the crew reaches Step 2 of AOP-018.

- If it is assumed that they assess the elapsed time to be less than 15 minutes, the crew will be directed to go to Step 10 of AOP-018 (Path 9) since there is no indication for them to believe that reactor coolant pump seal cooling cannot be restored in less than 15 minutes, and they will open FCV-626.
- However, if FCV-626 cannot be opened, since Step 2 is a continuous action step, the crew should keep track of the elapsed time since loss of seal injection while they continue in AOP-018. When the time runs out, they should go back to Step 2 and then transfer to Step 3 to trip the reactor coolant pumps.
- Otherwise, the crew would go to Step 3 from the Step 2 RNO column to trip the reactor coolant pumps (Path 10). Similar to Path 5, the crew will skip Step 10 when they continue in AOP-018, which is assumed to make the restoration of cooling by opening FCV-626 infeasible. Note that Step 5 of AOP-018 directs the crew to close FCV-626.



CAUTION

IF more than 15 minutes elapses without RCP Seal Cooling, THEN Seal Cooling (CCW AND Seal Injection) MUST be isolated before starting CCW OR Charging or Seal Damage could occur.

* 2.	Check Elapsed Time Since All RCP Seal Cooling Was Lost - GREATER THAN 15 MINUTES	IF RCP Seal Cooling is NOT OR can NOT be restored in less than 15 minutes, THEN Go To Step 3. Go To Step 10.
3.	Check Plant Status - MODE 1 OR MODE 2	Stop the affected RCP(s) Go To Step 5.

Figure D-4 Step 2 of AOP-018

D.3 Derivation of HEPs

D.3.1 Scenario Summary for Restoration of Seal Cooling by Opening FCV-626

Table D-1~~Table D-1~~ lists the possible scenarios for success and failure to open FCV-626. As mentioned at the beginning of Section 2, two procedure steps provide procedural guidance for the crew to open FCV-626. Scenarios 1 through 5 represents various procedural paths to these two steps. Among the five scenarios, Scenarios 2 through 5 differ in the procedural paths to AOP-018.

Note that Scenario 5 assumes that FCV-626 cannot be opened, which should have been in the PRA scenario and the relevant human failure event would be related to restoring seal injection.

Scenarios 6 and 9 represent a scenario class where the response is infeasible due to a timing constraint imposed by operating procedures. That is, regardless of which procedural path the crew takes to transfer to Section C of AOP-018, the response becomes infeasible if the elapsed time since loss of all seal cooling is more than 15 minutes when the crew reaches Step 2. This implies that the crew needs to move through the procedures fairly quickly; any delay would make the crew unable to open FCV-626.

Scenario 7 involves checking valve lineup upon recognition of loss of seal injection and then closing CV-310A to restore seal injection. If CV-310A can be closed, Path 7 is a success path for avoiding a seal LOCA by restoring seal cooling and thus precluding the need to open FCV-626. Given that instrument air is isolated from containment and identification of the issue with CV-310A relies on non-proceduralized sensemaking, closing the valve from the control room is considered infeasible (i.e., not credited in the HRA).

Similar to Scenario 7, Scenarios 4 and 8 also rely on non-proceduralized sensemaking to identify loss of seal injection. Scenario 8 assumes that the crew decides not to enter AOP-018 or APP-001-D1, thus it is considered infeasible because even though the reactor coolant pumps are tripped at Path-1 C11, opening FCV-626 to restore seal cooling from component cooling water is still necessary. The possibility of entering AOP-018 after tripping RCPs at Path-1 C11 is covered by Path 6 (i.e., Scenario 4).

Table D-1 Scenario Summary for HFE 3

Scenario No.	Procedural path	Scenario end status
1	Path 1	success
2	Path 2, Path 4, Path 9	success
3	Path 3, Path 4, Path 9	success
4	Path 6, Path 4, Path 9	success
5	Path 11, Path 4, Path 9	success
6	Path 5	infeasible
7	Path 7	infeasible
8	Path 8	infeasible
9	Path 10	infeasible

D.3.2 Scenario Summary for Tripping Reactor Coolant Pumps

Table D-2~~Table D-2~~ lists the possible scenarios of HFE 4. Scenarios 1 through 12 are combinations of the paths leading to AOP-018 and the paths to trip the reactor coolant pumps within AOP-018.

Scenario 14 involves checking valve lineup upon recognition of loss of seal injection and then closing CV-310A to restore seal injection. If CV-310A can be closed, Path 7 is a success path for the avoidance of a seal loss of coolant accident by restoring seal cooling and thus precluding the need to trip the reactor coolant pumps. Given that instrument air is isolated from containment and identification of the issue with CV-310A relies on non-proceduralized sensemaking, closing the valve from the control room is considered infeasible (i.e., not credited in the human reliability analysis).

Similar to Scenario 7, Scenarios 9 and 13 also rely on non-proceduralized sensemaking to identify loss of seal injection.

Table D-2 Scenario Summary for HFE 4

Scenario No.	Procedural path	Scenario end status
1	Path 2, Path 5	success
2	Path 2, Path 4, Path 10	success
3	Path 2, Path 4, Path 9	success
4	Path 3, Path 5	success
5	Path 3, Path 4, Path 10	success
6	Path 3, Path 4, Path 9	success
7	Path 6, Path 5	success
8	Path 6, Path 4, Path 10	success
9	Path 6, Path 4, Path 9	success
10	Path 11, Path 5	success
11	Path 11, Path 4, Path 10	success
12	Path 11, Path 4, Path 9	success
13	Path 8	success
14	Path 7	infeasible

D.3.3 Derivation of Total HEPs

For each scenario identified in Table D-1~~Table D-1~~and Table D-2~~Table D-2~~, a crew response diagram (CRD) can be developed and the human error probabilities assessed using the IDHEAS AT-POWER approach. These human error probabilities are conditional on the path chosen through the Scenario Map of Figure D-1~~Figure D-1~~. The total human error probability for each human failure event can then be evaluated as a weighted sum over the scenarios as follows:

$$HEP_T = \sum_i HEP_i * W_i$$

Where HEP_T is the total human error probability, HEP_i is the conditional human error probability for scenario I, and W_i is the probabilistic weight associated with scenario i. (i.e., it is the probability that the crew chooses scenario i). The weights would have to be based on discussions with the crew to try to determine their preferences based on their training and the conduct of operations.

D.4 Concluding Remarks

In this appendix we have presented a possible extension of the IDHEAS AT-POWER method to accommodate situations where the procedures do not provide a single, unambiguous success path. A key aspect of this approach is the development of the scenario map to identify significant decision points that are outside the scope of the cognitive activities addressed by the crew failure modes of IDHEAS AT-POWER. Implementation of this approach would require the analyst to assess the relative likelihoods of following the various paths identified based on an

understanding of the crew practices and training. This approach can also provide input to the assessment of the dependence between the two human failure events since the success paths are intertwined and at least a portion of the paths are common to both responses.

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG-2199, Vol. 3

2. TITLE AND SUBTITLE

Testing the Integrated Human Event Analysis System for Nuclear Power Plant Internal Events At-Power Application (IDHEAS AT-POWER)

Volume 3

3. DATE REPORT PUBLISHED

MONTH	YEAR
~~May~~	~~2022~~

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

H. Liao, S. Morrow, G. Parry, M. Presley, L. Criscione, D. Bley

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Same as above

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This report documents a study of the Integrated Human Event Analysis System for nuclear power plant internal events at-power application (IDHEAS AT-POWER), a human reliability analysis method developed by the U.S. Nuclear Regulatory Commission and the Electric Power Research Institute. The purpose of the study was to perform a holistic test of the method to identify strengths and weaknesses. Five analyst teams applied the method to analyze five predefined human failure events for three scenarios in a pressurized water reactor. The study evaluated the method against five criteria: validity, interanalyst consistency, traceability, usability, and utility. The results indicated that IDHEAS AT POWER provides a structured analysis framework and traceable quantification approach to HRA. However, there was variability in the results between analyst teams, particularly in the assessment of execution tasks and credit for recovery. The report presents a discussion of the strengths and weaknesses of IDHEAS AT-POWER, lessons learned from the study, recommendations for improvement in the method guidance, and suggestions for future method development.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Human reliability analysis
Human error probability
Nuclear power
Human performance
Performance influencing factors

13. AVAILABILITY STATEMENT

unlimited

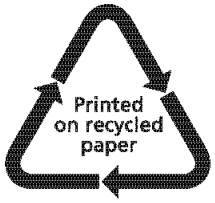
14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE



Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS