

Example Application of Model-Based HRA Approach

Song-Hua Shen^a, Ali Mosleh^b, Dana L. Kelly^c, Ronald L. Boring^c,

^aUS Nuclear Regulatory Commission, Washington, DC, USA

^bUniversity of Maryland, College Park, MD, USA

^cIdaho National Laboratory, Idaho Falls, ID, USA

Abstract: In response to a Staff Requirements Memorandum (SRM) to the Advisory Committee on Reactor Safeguards (ACRS), the US Nuclear Regulatory Commission (NRC) has undertaken a research effort to create a consensus approach to human reliability analysis (HRA). The qualitative part of the approach includes a scenario-driven method of capturing possible interactions of the operating crew with the plant. At its top-layer, the method includes a Crew Response Tree (CRT) that identifies human failure events (HFEs). The potential failure mechanisms of the HFEs are explored with the aid of a mid-layer “causal model” using the Information-Diagnosis/Decision-Action (IDA) model and cognitive models from the psychological literature. The last layer of the model links relevant performance shaping factors (PSFs) to each failure mechanism. These layers together embody the results of task analysis and evaluation of context factors performed by an interdisciplinary team of analysts. In each scenario of the CRT, the mid-layer and bottom-layer models are linked together to produce the sequence of events and their causes that lead to one or several HFEs. Two companion papers in this conference proceedings describe the overall methodology and the development of the mid-layer models. This paper presents an illustrative application of the method.¹

Keywords: HRA, Failure Mechanism, IDA, Qualitative Analysis.

1. INTRODUCTION

In a Staff Requirements Memorandum (SRM) to the Advisory Committee on Reactor Safeguards (ACRS) [1], the US Nuclear Regulatory Commission (NRC) directed the ACRS to “work with the staff and external stakeholders to evaluate the different human reliability models in an effort to propose a single model for the agency to use or guidance on which model(s) should be used in specific circumstances.” As a first step toward meeting this directive, an effort has been undertaken to develop a comprehensive qualitative analysis approach for human reliability analysis (HRA). The proposed approach uses two modeling vehicles: (1) a process and representational method for analyzing crew-plant interactions, focusing on identifying and quantifying human failure events (HFEs) and recovery, and (2) a model of human response relating the observable human (crew) “failure modes” to “context factors”. The first modeling tool is a forward-branching tree of operator (crew) cognitive activities and actions (Crew Response Tree, CRT). CRT provides a causal explanation of the HFEs that will appear in the PRA event trees or fault trees (see Figure 1 and refer to [1] and [2] for more details). Depending on whether the unit of analysis is the crew or individual operators, the “branch points” of the CRT can include operator action options, operator decision options, crew member interactions, and key plant functional states. CRT is developed by an interdisciplinary team of PRA analysts as it requires knowledge of plant behavior and human response. Instances of possible human failure events that are identified within these CRTs are then explored further in supporting fault trees that help identify failure mechanisms (within a fault tree logic) underlying the human failure events. A final step is the identification of relevant performance shaping factors (PSFs) driving the identified failure mechanisms.

¹ The information presented in this paper does not currently represent an agreed-upon NRC staff position. The NRC has neither approved nor disapproved its technical content.

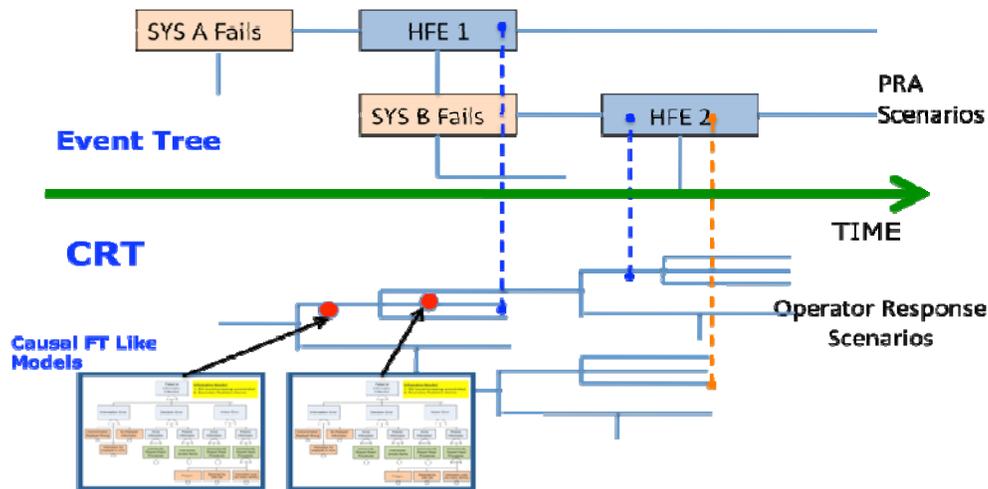


Figure 1. Operator-Plant Interaction Scenario Modeling through CRT and Causal Fault Trees

The layers of models together embody the results of task analysis and evaluation of context factors performed by an interdisciplinary team of analysts. In each scenario of the CRT, the mid-layer and bottom-layer models are linked together to produce the sequence of events and their causes that lead to one or several HFEs. Two companion papers in this conference proceedings describe the overall methodology [2] and the development of the mid-layer fault trees models [3]. This paper presents an illustrative application of the method. We first describe the key steps of the analysis (including general rules for building CRTs) and then provide a simple illustrative example. Many features and steps of the analysis methodology are in the developmental stage and are likely to change during various conceptual and implementation iterations, model integration, and testing.

2. ANALYSIS PROCEDURE

The analysis procedure includes several key steps: (1) construction of the CRT, (2) development of causal factors at CRT branch points via mid-layer fault trees, (3) linking mid-layer models and corresponding PSFs through the logic of the various CRT scenarios and branch points, (4) solving the resulting linked model to obtain crew-plant interaction scenario “cutests”. In all steps qualitative and quantitative screening of unlikely scenarios and contributing factors and use of merge rules common in PRA help limit the size of the models and the number of scenarios that need to be analyzed.

2.1 Constructing CRTs

CRT is an analysis aid to ensure systematic coverage of crew-plant interactions consistently with the scope of the analysis. As such, the CRT identifies the opportunities for and types of HFEs in the context of an accident or plant upset. We note that event trees essentially play a similar role in PRA, although the level of resolution is normally inadequate for HRA analysis. CRTs are also envisioned as an HRA work product, a means of documenting and reporting HRA analysis. Each sequence of events (decisions, actions, HFE, recovery action, etc.) in the CRT is a pictorial representation of a possible crew response scenario in the entire accident (from initiation to termination).

The development of the CRT and PRA Event Tree is an iterative and collaborative process conducted by a multi-disciplinary team. CRT will normally carry much more information than typical event trees, and embodies the integrated picture of the plant-crew interactions. Normally, one CRT is developed for each PRA event tree. The level at which the two models interface are the crew actions that directly impact the evolution of the plant scenarios (as viewed through the eyes of the event tree). Accordingly, at interface points, both CRT and ET should have the same level of abstraction or details (for instance, in defining equipment boundaries and HFEs). The CRT and the ET will have the same

starting point in time and physical state, namely the Initiating Event. CRT and ET share the same event timeline, and time is as a minimum an implicit parameter in both trees.

EOPs and similar procedures are used as a guide to develop the nominal scenarios in the CRT. Corresponding Decision Points and Action Opportunities are used to identify “branch points” of the CRT. CRT branch points should determine “modes” of response (e.g., failure or success) from a “functional” point of view (e.g., “failure to close a valve”). The “functional response mode” is defined at a level consistent with the PRA (ET and FT) level of detail, but failures are not necessarily identical to the HFEs as they appear on the event tree (for example, they could simply be “contributing causes of the HFE”).

The key steps are as follows:

1. **Identify the Initiating Events:** By definition, an initiating event is the beginning point in the abnormal sequence. This step is the same as the identification of the initiating event for PRA event trees.
2. **Define the Safety Function:** Similarly to process of developing conventional event trees, the following safety functions are considered in the CRT development: Reactivity Control, Reactor Coolant System Inventory Control, Reactor Coolant System Pressure Control, Core Heat Removal, Reactor Coolants System Heat Removal, Containment Isolation, Containment Temperature and Pressure Control. Some of the safety functions are not explicitly modeled in current PRA event tree, but may still affect the operators’ mental states. For instance, Safety Injection is not explicitly modeled in the SGTR event tree; however, its automatic or manual actuation may impact operator performance.
3. **Delineate the Accident Sequences:** Delineates the abnormal sequence in accordance with the event tree model and all relevant safety functions.
4. **Construct the CRT for each identified function:** Procedures need to be reviewed step by step in a detailed task analysis process. At each step, all the major decisions and/or actions are considered. These are candidates for inclusion in the CRT. The CRT joins similar steps to create a simplified representation of the task analysis, and is designed primarily to identify and model the HFEs, although some non-HFE steps may also be modeled for context. Note that the CRT is meant as a complement to the detailed task analysis, and the task analysis should be thoroughly documented as supplemental analysis material.

The following are examples of branch points to consider during construction of CRTs.

- Success path—What the operators do to ensure the safe functioning of plant systems (top line of tree)
- Failure path—What may compromise the safe functioning of plant systems (bottom line(s) of tree)
- Human-caused failure
- Hardware-caused failure (we do not model hardware-only failures in the CRT, but rather hardware that triggers human failures)
- Procedural cautions serve as a useful information source for both human-caused and hardware-caused failures
- Opportunities to branch to another procedure (kick-outs)
- Other paths observed from operations experience, including simulator studies used as inputs to the task analysis (deviation path)

Clustering rules help reduce the number of CRT scenarios. The “clustering rules” below guide the grouping process. Each group corresponds to a branch point in the CRT.

- Outcome: Actions/decisions related to the same functional effect on a system (e.g., multiple steps to isolate SG) should be clustered
- Intent: Actions/decisions related to same goal (e.g., checking indicators for overall symptoms) should be clustered

- Significant obstacles to goal completion (e.g., unreliable indicators) should be modeled as failure paths. Failure paths may pertain to the entire cluster or to subtasks within a cluster.
- Cause: Actions/decisions that share common failure mechanisms may be clustered
- Cognition: Actions/decisions that are part of a common cognitive flow (e.g., related D and A subparts) should be clustered rather than treated as separate processes
- Dependence: Actions/decisions that are moderately or highly dependent at the subtask level may be clustered
- Where HFEs are provided, this may serve as the logical clustering mechanism (e.g., a series of procedural steps may all relate to the same HFE, in which case they are captured as a single branch point)

Many procedural steps include a list of substeps the operator should perform. As a general rule, these substeps are not modeled in detail. However, if a substep reveals an opportunity for human failure, this failure path should be modeled in the overall branch point. Substeps may be clustered in the same manner as procedural steps. The level of decomposition should correspond to the PRA (e.g., if the PRA specifies system or component level failure, the CRT should model to this level of human interaction with components). Paths that are deemed of low likelihood or not risk significant may be excluded from modeling in the CRT.

2.2 Tailoring and Linking Mid-layer Fault Trees to CRT

The next step is to use the generic fault trees of the mid-layer model (See Ref [2]) to give causal depth to the CRT branches, where human deviations from the nominal path are indicated. For each branch point, the generic tree may need to be tailored by deleting logic gates or basic events that are not relevant to the specific situation represented by the CRT branch point.

3. AN EXAMPLE

During the SGTR event, secondary heat sink is a necessary safety function to remove the heat generated from the core, given successful reactor trip and safety injection. According to the system design, the AFW is the primary “secondary heat sink.” If the AFW fails, MFW may be restored as a back-up secondary heat sink. If both MFW and AFW fail, “feed and bleed” is the final option to prevent core damage. A typical ET for this case is shown in Figure 2.

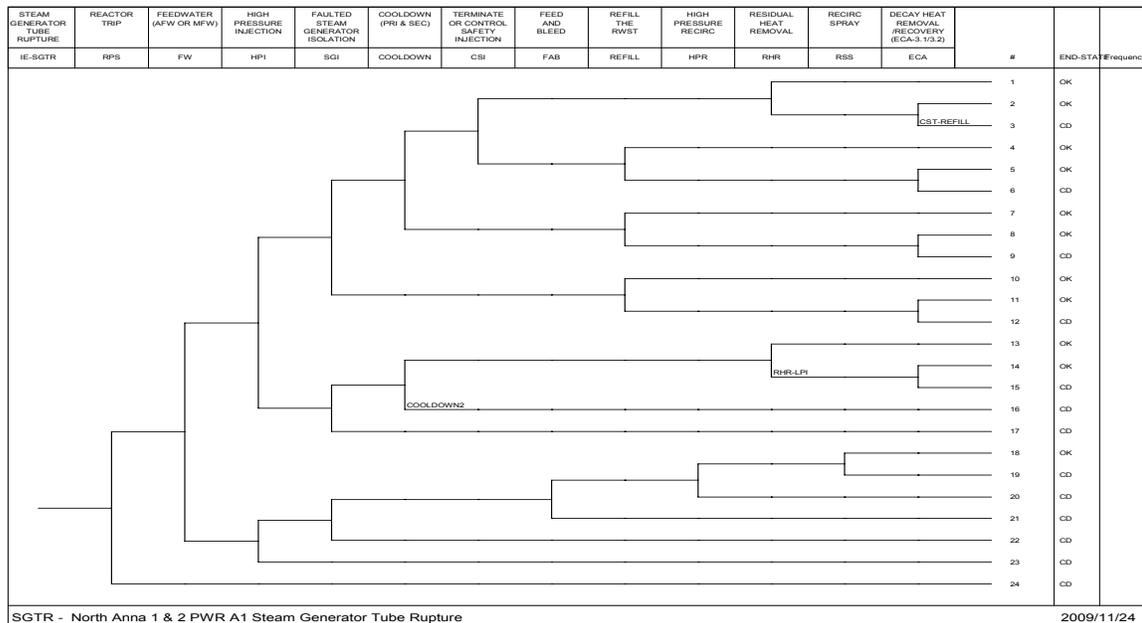


Figure 3 Simplified CRT for Example Case

Even if the operators enter the EOP FR-H.1, they may still quit this procedure (eleventh branch point) if they assess the plant condition incorrectly during step 1 of the EOP FR-H.1. If, however, the operators assess the plant condition correctly, step 2 directs them to restore the AFW (twelfth branch point). Because the twelfth branch point is conditioned on the AFW system's availability, if the operators fail in this simple task, we will assume that they are unlikely to succeed in more complicated tasks such as restoring MFW and F&B, and this failure path ends with core damage (simplification for this example).

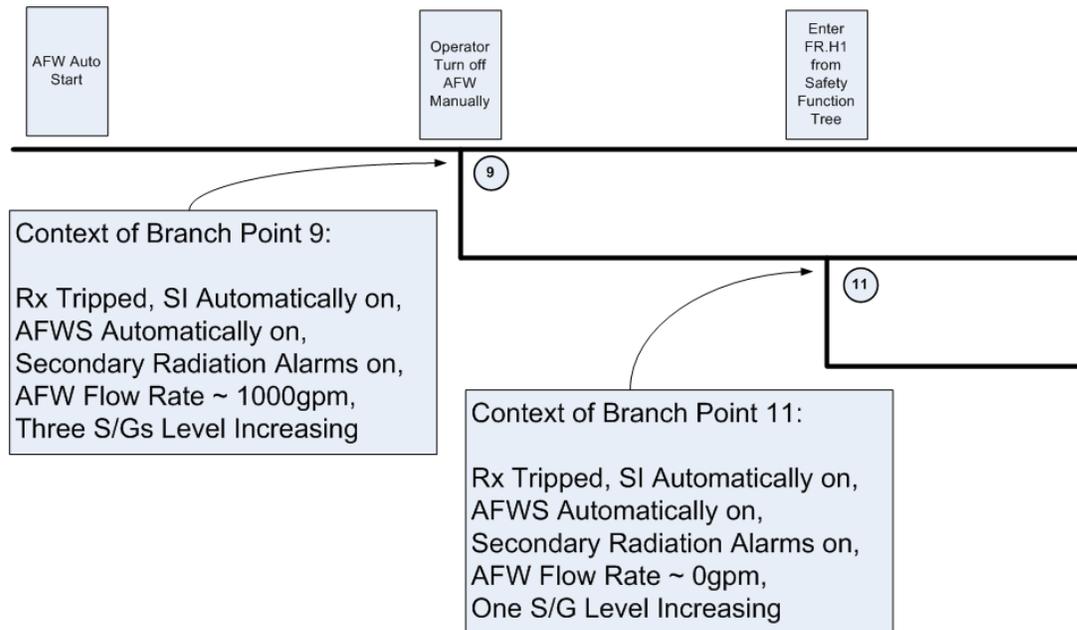


Figure 4. Portion of CRT of Figure 3 Selected for Further Analysis

3.2 Linking Causal Fault Trees

Next we tailor the generic mid-layer fault trees (see Ref [3]) for use in the CRT of Figure 3. We will do this only for a subset of the CRT scenarios. This portion is shown in Figure 4. Some of the key scenario features are listed in the text boxes for each Branch Point (B9 and B11). The parts of the mid-layer causal fault trees that apply to these branches are identified by the thicker lines in the various fault trees in Figure 5-a through 5-d. These modified fault trees are linked to CRT and solved to obtain the cut-sets (combination of failure causes and mechanisms) that contribute to Sequence 1

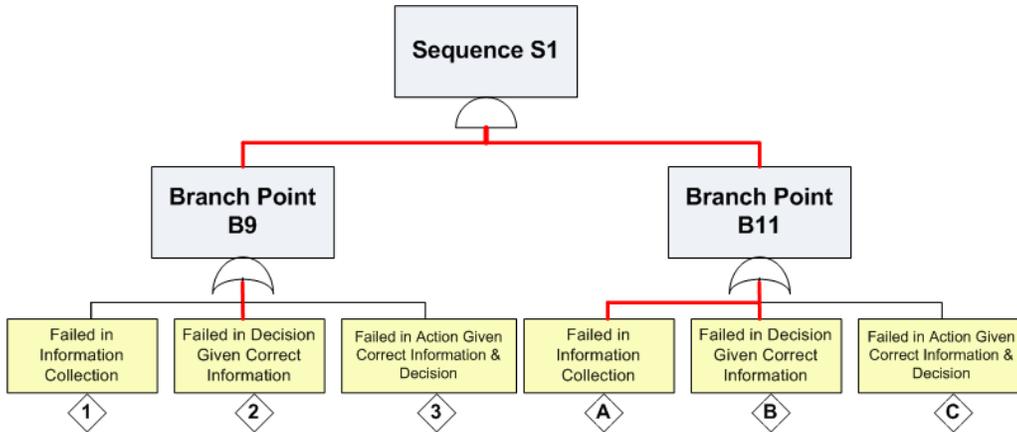


Figure 5-a Tailored Mid-Layer Fault Trees Linked for Sequence 1 of Example CRT

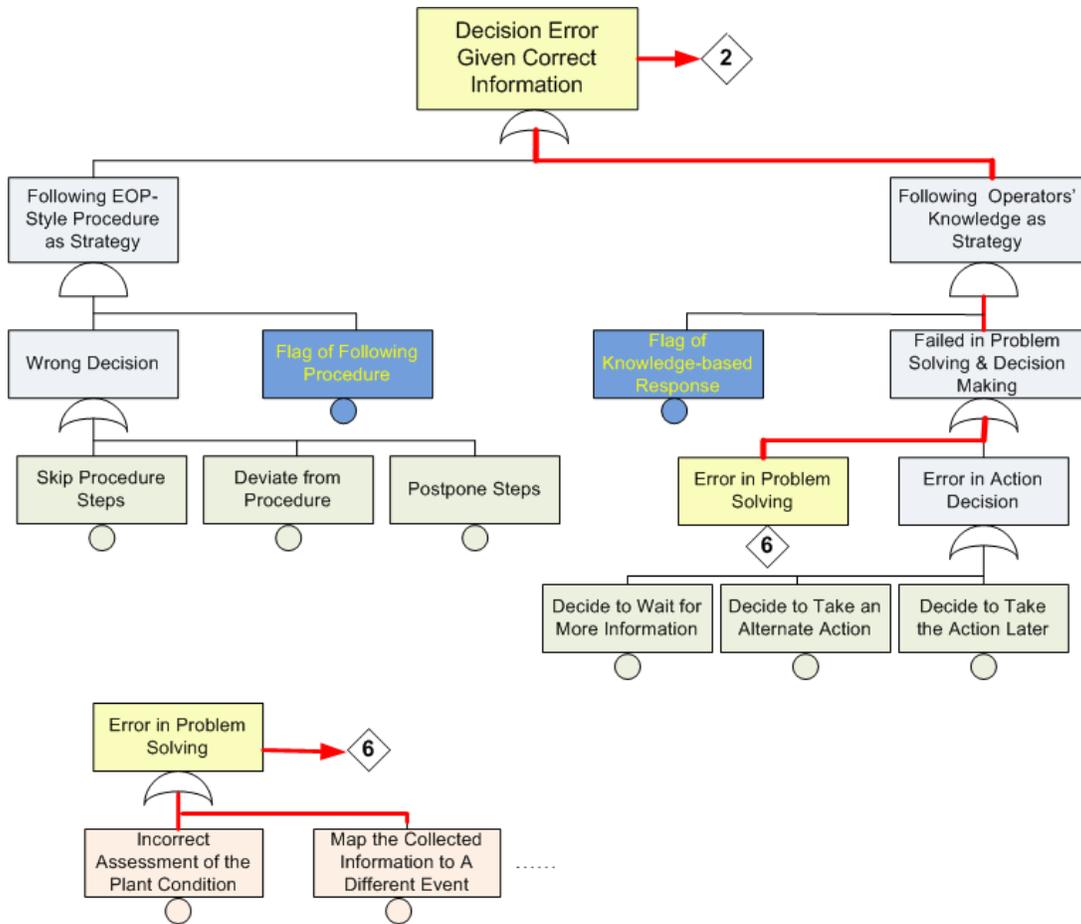


Figure 5-b Tailored Mid-Layer Fault Trees for Example CRT

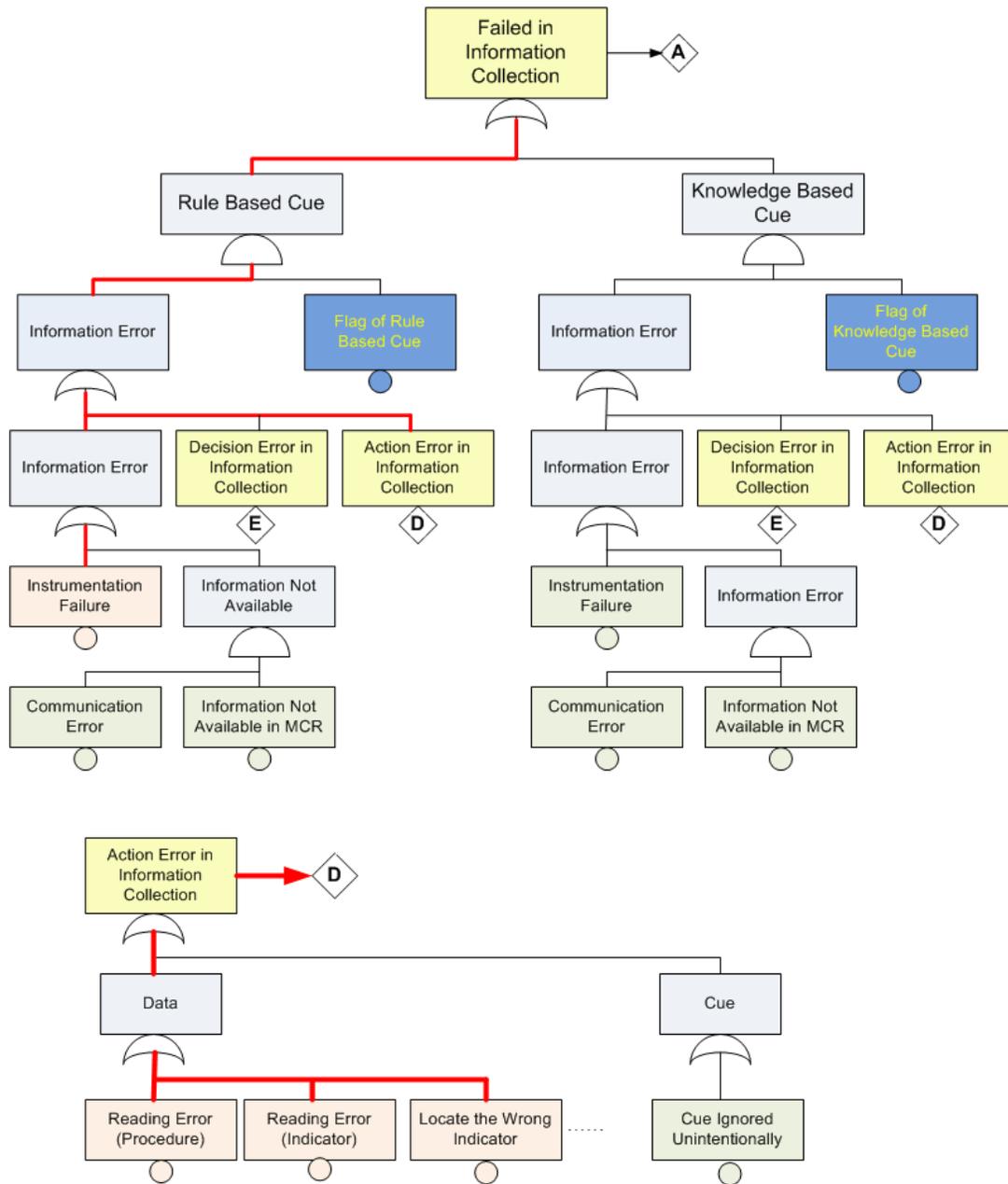


Figure 5-c Tailored Mid-Layer Fault Trees for Example CRT

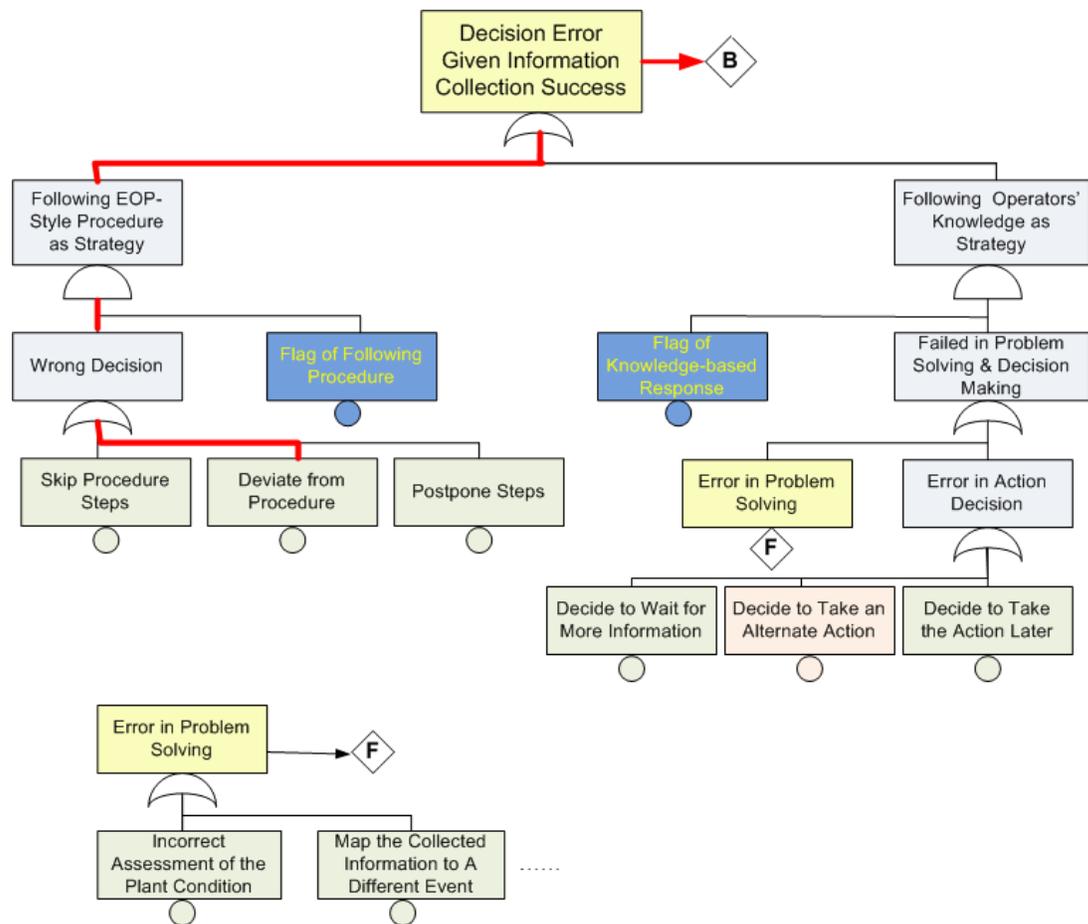


Figure 5-d Tailored Mid-Layer Fault Trees for Example CRT

3.3 Analysis of Scenario S1

The underlying plant scenario of Sequence S1 is as follows:

- S/G U-tube Ruptured
- Secondary Radiation Alarms on
- One S/G level increasing
- S/G High Level Tripped Turbine, and then Rx automatically Tripped, SI Automatically on
- AFWS Automatically on
- AFW Flow Rate ~ 1000 gpm
- Three S/Gs Level Increasing

In Branch Point B9, the operators manually trip the AFW system. STA is monitoring the Critical Function Tree. When the Critical Function Tree “red path condition” is met, STA instructs the operator to enter FR-H.1 procedure. The operator enters FR-H.1, step 1 to check whether the secondary heat sink is required. If the operator determines that the secondary heat sink is not required, he transfers back to E-0, and the path leads to core damage because of the lack of the secondary heat sink.

Left hand side of mid-layer fault tree of Figure 5.a (for Branch Point B9) models the failure mechanisms that may lead the operator to turn off the AFW system manually. Right hand side of mid-

layer fault tree of Figure 5.a (for Branch Point B11) models the failure mechanisms that may lead the operator to determine that the secondary heat sink is not required.

The relevant paths in both sides of FT of Figure 5.a are highlighted, and further linked to fault trees in Figure 5.b, 5.c, and 5.d. for specific failure mechanisms that apply in this situation (context of Scenario 1). According to the context of branch point B9, because of the increasing S/G level, the operator may turn off the AFW system to prevent the S/G and steamline from going solid. Checking the failure modes under fault tree B9, “Assess the Plant Condition Incorrectly ” and “Map the Collected Information to a Different Event” are two likely failure modes to lead this **commission error**. All other failure modes, such as the “instrumentation error” or “action error”, are not relevant to this human failure.

Table 1 is the list of Scenarios 1 cut-sets generated for the linked fault tree of Figure 5.a. In these cut-sets, the basic event names starting with B1_ designate failure modes from the Branch Point B9, while the basic events starting with B2_ are the failure modes from Branch Point B11.

In pruning the CRT, generic fault tree segments generating low likelihood or irrelevant events, are set to zero. Probabilities need to be evaluated on the basis of a quantification methodology that allows factoring in the effect of context factors such as PSFs. Since the focus of this example is the qualitative analysis, a value of 10⁻³ is used for all other basic events. The probabilities of “Assess the Plant Condition Incorrectly” and “Map the Collected Information to A Different Event” are set to 1.0E-3. Probabilities of all other failure modes are set to zero.

Possible scenarios are reflected in the cut-sets. For example, the first cut-set (table 1) represents the operators incorrect assessment of the plant condition and subsequent decision to turn off the AFW system (Assess the Plant Condition Incorrectly), getting the wrong information by checking a wrong indicator when performing step 1 of FR-H.1, and quitting he FR-H.1 procedure (Choose the Wrong Indicator).

The PSFs and other context factor that make this scenario more or less likely are not included in this example analysis because the corresponding modeling steps and analysis procedure are still under development.

Table 1 Causal Cut-sets Generated for Example Sequence 1

#	Prob/Freq	Cut Set	Description
1	1.00E-03	B1_D_KATPCW	Assess the Plant Condition Wrong
	1.00E-03	B2_R_CTWI	Choose the Wrong Indicator
2	1.00E-03	B1_D_KATPCW	Assess the Plant Condition Wrong
	1.00E-03	B2_R_REP	Reading Error (Procedure)
3	1.00E-03	B1_D_KATPCW	Assess the Plant Condition Wrong
	1.00E-03	B2_R_REI	Reading Error (Indicator)
4	1.00E-03	B1_D_KATPCW	Assess the Plant Condition Wrong
	1.00E-03	B2_R_IF	Instrumentation Failure
5	1.00E-03	B1_D_KATPCW	Assess the Plant Condition Wrong
	1.00E-03	B2_D_P_DFP	Deviate from Procedure
6	1.00E-03	B1_D_K_MTCITADE	Map the Collected Information to A Different Event
	1.00E-03	B2_R_CTWI	Choose the Wrong Indicator
7	1.00E-03	B1_D_K_MTCITADE	Map the Collected Information to A Different Event
	1.00E-03	B2_R_REI	Reading Error (Indicator)
8	1.00E-03	B1_D_K_MTCITADE	Map the Collected Information to A Different Event
	1.00E-03	B2_R_REP	Reading Error (Procedure)
9	1.00E-03	B1_D_K_MTCITADE	Map the Collected Information to A Different Event
	1.00E-03	B2_R_IF	Instrumentation Failure
10	1.00E-03	B1_D_K_MTCITADE	Map the Collected Information to A Different Event
	1.00E-03	B2_D_P_DFP	Deviate from Procedure

Acknowledgements and Disclaimers

This work was funded by the U.S. Nuclear Regulatory Commission (USNRC) at Sandia National Laboratories (Sandia) and Idaho National Laboratory (INL). Sandia is a multi-program laboratory operated by Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000. INL is a multi-program laboratory operated by Battelle Energy Alliance, for the United States Department of Energy. The University of Maryland participated under subcontract from Sandia. This work of authorship was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government, nor any agency thereof, nor any of their employees makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately-owned rights. This paper was prepared in part by employees of the USNRC. It presents information that does not currently represent an agreed-upon staff position. NRC has neither approved nor disapproved its technical content.

References

- [1] US Nuclear Regulatory Commission, *Staff Requirements—Meeting with Advisory Committee on Reactor Safeguards, SRM M061020*, US Nuclear Regulatory Commission, November 8, 2006, Washington, DC.
- [2] A. Mosleh, J.A. Forester, R.L. Boring, S. Hendrickson, A.M. Whaley, S.H. Shen, D.L. Kelly, J.Y.H. Chang, V. Dang, J.H. Oxstrand, and, E.L. Lois, “*A Model-based Human Reliability Framework*”, Proc. of the 10th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM10) (this conference).
- [3] S. Hendrickson, A.M. Whaley, R.L. Boring, J.Y.H. Chang, S.H. Shen, A. Mosleh, J.H. Oxstrand, J.A. Forester, D.L. Kelly, E.L. Lois, “*A Mid-Layer Model for Human Reliability Analysis: Understanding the Cognitive Causes of Human Failure Events*”, Proc. of the 10th Int. Conf. on Probabilistic Safety Assessment and Management (PSAM10) (this conference).