SAND2012-1302C

A Model-Based Approach to HRA: Qualitative Analysis Methodology

Johanna Oxstrand[a*], Dana L. Kelly[a], Song-Hua Shen[b], Ali Mosleh[c], Katrina M. Groth[d]

[a] Idaho National Laboratory, Idaho Falls, USA
[b] US Nuclear Regulatory Commission, Washington DC, USA
[c] University of Maryland, College Park, USA
[d] Sandia National Laboratories, Albuquerque, USA

Abstract: This paper describes a model-based approach to the qualitative portion of Human Reliability Analysis (HRA). The goal of the qualitative analysis approach is twofold: 1) to incorporate salient information from the cognitive psychology literature into the analysis, and 2) to develop models and guidance to support analysis teams as they gather and organize the information needed for the follow-on quantitative portion of the HRA. A focus in the development has been to provide guidance and assistance for HRA analysts with a wide range of skill levels. This is because the growth in risk-informed applications has demanded that analysts who are not experts in cognitive science must use HRA methods to generate inputs to risk-informed decision-making. The qualitative analysis approach is also intended to be generic in the sense that it should be compatible with various quantification methods. Tools have been developed as a part of this approach to qualitative analysis, particularly the Crew Response Tree (CRT) and Fault Trees for causal delineation. The Crew Response Tree provides a structured way to identify, define, and decompose Human Failure Events in the HRA. Together with the CRT, the Fault Trees provide the structure needed to enhance consistency and traceability in the qualitative analysis. The Fault Trees are designed to guide the analyst in identifying the ways in which plant crews can fail. They represent a simplified model of human cognition in the nuclear power plant domain and have been explicitly linked to currently accepted psychological/cognitive models. This set of tools – the CRT and the Fault Trees – provides enhanced traceability of the HRA analysis since documentation is inherent in the tools.

Keywords: HRA, Crew Response Trees, Fault Trees, Cognitive Model

1. INTRODUCTION

A companion paper by Mosleh et al [1] describes a model-based methodology for human reliability analysis (HRA). The proposed framework includes concepts and techniques for both the qualitative and quantitative parts of HRA, aiming to address a number of key issues with current methods. This paper provides more details on the qualitative part of the methodology. The goal of the qualitative analysis methodology is twofold: 1) to incorporate salient information from the cognitive psychology literature into the analysis, and 2) to develop models and guidance to support the analysts as they gather and organize the information needed for the follow-on quantitative portion of the HRA. It has long been recognized that variability in the qualitative portion of the HRA is a significant contributor to variability in the quantitative results of the HRA. This was most recently noted in the International HRA Empirical Study (Lois, et al., 2009). Thus, the main goal of this effort has been to reduce unexplained or opaque variability in such a way that the sources of any remaining variability are readily apparent. An ancillary benefit is that the methodology should provide a better foundation for using the qualitative analysis to reduce human errors in the operation of complex systems.

A focus in the development has been to provide guidance and assistance for non-expert HRA analysts. This is because the growth in risk-informed applications has demanded that analysts who are not experts in HRA must nonetheless use quantitative HRA methods to generate results that feed into risk-informed decision-making. The qualitative analysis methodology is also developed to be generic in the sense that it should be compatible with most HRA quantification methods.

The HRA methods that are most commonly used today are not consistent with regards to the qualitative analysis required, with some (e.g., SPAR-H) providing no guidance for the qualitative analysis. There is also inconsistency at the level of task decomposition (note that the ASME/ANS PRA Standard requires task decomposition in certain applications). As noted above, this inconsistency causes variability in the human error probabilities (HEP) produced by quantification. Lack of a common task decomposition framework can also lead to inconsistency in the unit of analysis for quantification. The level of task decomposition also affects assessment of dependency between tasks, which further influences the HEPs. The ISPRA study of the 1980s found that even with commonly defined human failure events (HFE), there was considerable variability in how analysis teams modeled the HFE. Differences in task decomposition played a significant role in the differences among the HEPs for the HFEs (Boring, Forester, Bye, Dang, & Lois, 2010). Hence, there is a need for a structured way to identify, define, and decompose HFEs in the HRA. The qualitative analysis methodology described in this paper includes two tools developed with this goal in mind: the Crew Response Tree (CRT) and Fault Trees.

This paper will describe the qualitative analysis methodology in detail. A companion paper (Groth et al, 2012) describes an example of how to apply the methodology. The CRT and Fault Trees provide enhanced traceability of the HRA analysis since documentation is inherent in the tools. This approach to the qualitative analysis is a step forward in linking HRA with human factors and providing a structured way in which to conduct the qualitative analysis.

2. THE HRA QUALITATIVE PROCESS

It is common to assume that the starting point for the qualitative analysis is defined HFEs, which are a result of an iterative process of developing PRA scenarios. The set of HFEs should represent those needed to model the impact of potential human failures on the accident scenario progression. If it is assumed that the starting point of the qualitative analysis is the set of identified HFEs, the qualitative analysis can be described generically as a four-step process: 1) Refinement of HFE Definition, 2) Task Analysis, 3) Identification of Failure Causes, and 4) Assessment of Influence of Context.

Refinement of HFE Definition: The first step in the qualitative analysis is to refine the definition of the HFE. The analyst needs to understand the scenario and the context that affects it. The analyst also needs to understand which procedures, intended and otherwise, the crew might use in the specified scenario. Most HFEs comprise two or more procedural steps. Therefore, some sort of HFE decomposition is useful to represent procedural flow.

Task Analysis: This part of the qualitative analysis identifies the subtasks associated with the operator actions related to the specific HFE. The task analysis also supports the identification of opportunities for incorrect responses, along with opportunities to recover from an incorrect response.

Identification of Failure Causes: The third step of the qualitative analysis is to identify the potential causes for human errors that could lead to failure of the specific HFE.

Assessment of Influence of Context: The final step of the qualitative analysis identifies and assesses the strength of factors that influence the likelihood of the failure causes. These factors are derived from the context provided by plant, scenario, and crew conditions. These factors can raise or lower the likelihood of failure via the associated failure causes.

The CRT is a tool for task decomposition (typically along procedural lines). The CRT supports the first three steps in the qualitative analysis. However, in most current human reliability assessments it is assumed that the Human Failure Event is already defined. In these cases the first step in the qualitative analysis process described above will not be applicable. The Fault Trees developed for this specific HRA methodology will guide the analyst to identifiy the specific nature of the failure causes as well as the context in which the failures occur. While developing the CRT the analyst identifies critical paths, i.e. paths in the CRT that the analysts decide are of interest for further analysis. The branch points in these paths will be analyzed by the Fault Trees to identify the Crew Failure Modes (CFM) associated to each branch point. The Performance Influencing Factors (PIF) corresponding to each CFM will be identified through the application of Bayesian Belief Networks. The critical paths and their associated CFMs and PIFs are the bases for the quantification of human error probabilities. Table 1 describes the 6 steps in the proposed methodology for qualitative analysis.

Table 1. The Qualitative Analysis Methodology Process

	Step	Description
1	Human Failure Event Identification	The HRA/PRA team review Event Sequence Diagrams, Event Trees, etc to identify relevant HFE(s).
2	Scenario Familiarization	The analysts read and get familiar with the scenario related to the HFE(s). This includes plant visits and other activities to gather information on what, how, and why the scenario might evolve as described.
3	Procedure Identification	Based on the scenario descriptions the analysts identify the safety functions involved. For each safety function the analysts need to identify the procedures the operating crews might use to successfully initiate the safety function.
4	Crew Response Tree construction	By stepping through the CRT Flowchart the analysts constructs a CRT for each of the identified safety functions.
5	Critical Path Identification	Based on the understanding of the scenario, the information captured during the complete qualitative analysis, and based on the analyst's understanding of the PRA scenario the analysts' identifies the critical paths in the CRT.
6	Crew Failure Mode and Performance Influencing Factors Identification	By applying the Fault Trees for each of the critical paths in the CRT the analysts will be able to identify the relevant Crew Failure Modes (CFM). Each CFM is associated with Performance Influencing Factors identified by using a Bayesian Belief Network.

2. THE CREW RESPONSE TREE

The Crew Response Tree is a tool to identify both the functional failures and the contextual information that are relevant to the development of the scenario/HFE. Based on the HFE, the analyst will identify the safety function(s) that play a main role. Examples of safety functions include "Steam Generator Isolation" and "Auxiliary Feed Water". The safety functions are commonly found in the error trees used in the PRA. The HRA team needs to review the error trees and consider other gathered information regarding the HFE to decide what safety function to analyze. Sometimes there is more than one safety function driving the behavior of the HFE. One CRT will be developed for each identified relevant safety function. These function-based CRTs may be linked to cover the full range of an accident time line and possible scenarios as reflected in corresponding PRA event tree or event sequence diagram. The CRT provides a framework to decompose the safety functions. Via this decomposition, the CRT identifies deviation pathways as well as critical paths (i.e., paths that lead to the failure of the safety function). These deviation paths could aid in identification of new HFEs, enhancing completeness of the PRA/HRA. The CRT also supports the analyst in identifying where additional information is needed to reach completeness in the qualitative analysis, such as timing information from simulator observations to determine if a path through the CRT leads to failure. The CRT also provides a graphical representation of the entire task analysis, enhancing traceability. The CRT is both an easily reviewed representation of procedural flow and a helpful aid for identification of subtasks to analyze in more detail.

The construction of the CRT is an exercise in structured task decomposition and should be conducted according to the guidance provided in the CRT Flowchart, described and discussed later in this document. The construction of a CRT should result in more consistent task decomposition without excessive effort.

The handoff to the Fault Trees happens when the CRT is fully created. Using the context provided in the CRT, the PRA model, PRA expertise, and HRA expertise should identify critical paths in the CRT. These critical paths are the candidates for more detailed analysis and quantification. The CRT provides a first cut of the boundary conditions for linking to the quantitative portion of the HRA.

3.1. CRT Flowchart

A CRT is primarily constructed to represent the task decomposition. A CRT Flowchart is proposed in this paper to support the analyst in constructing the CRT. Hence, the CRT Flowchart is to be viewed as the procedure aiding the analyst in the CRT development process. The questions in the flowchart guide the addition of branches to the CRT. Hence, the flowchart has pruning rules incorporated into its design. The input to the CRT and the output are summarized in Table 2.

Table 2. The Input Needed to Construct a CRT and the Output From the CRT

Input	**Output**
HFE definition Identified Safety Function Plant context Crew context Procedures used in the to complete/conduct the Safety Function (including alternative procedures the crew might employ)	A task decomposition of the safety function in the form of a tree, which can be used to find the paths and branch points of interest for quantification.

Before starting the process of constructing a CRT for the specified HFE, the analysts must have the HFE definition provided by the PRA. The analysts also need information regarding other contextual factors that might influence the crew while responding to the PRA scenario involving the specified HFE. This information can be gleaned from operator and analyst experience, simulator observation, etc. It is recognized that the analyst cannot be assumed to have a complete set of information needed to properly construct the CRT before starting the construction process. The analyst is encouraged to collect additional information as needed during the process. The analysts also need to know which procedures will be used in the specific scenario, including possible alternatives that the crew might employ, perhaps in error. Although the CRT represents procedurally driven task decomposition, and thus would appear to be applicable only for internal events occurring at full power, where most of the tasks represented in the CRT involve Emergency Operating Procedures (EOPs) related to the scenario, the CRT can also be employed for other scenarios less closely linked with EOPs.

Based on the understanding of the contextual factors and the HFE definition, the analyst steps through the CRT flowchart to construct the CRT, beginning with the first question that asks whether the specific function is designed to be initiated automatically. If the answer is yes, the analyst would follow the Yes-arrow to question number 2: “Is the scenario a fast transient?” If the answer is no, the analyst will follow the No-arrow to the box which say “Branch Point A”. This informs the analyst that one branch point in the CRT should be created. The branch point’s success path is the operator manually initiated the safety function before it is automatically initiated. The failure path is the operator does not manually initiate the safety function. When the branch point is added to the CRT the analyst continues to follow the CRT Flowchart. The CRT will be fully created when the analysts reach the sixth and final question in the CRT Flowchart: “Is there extra equipment and manual actions which may perform the specific safety function?” If the answer is no, the process of constructing the CRT is complete.

Figure 1 below shows the CRT Flowchart. Table 3 and 4 provide detailed description of the questions and branch points in the CRT Flowchart.

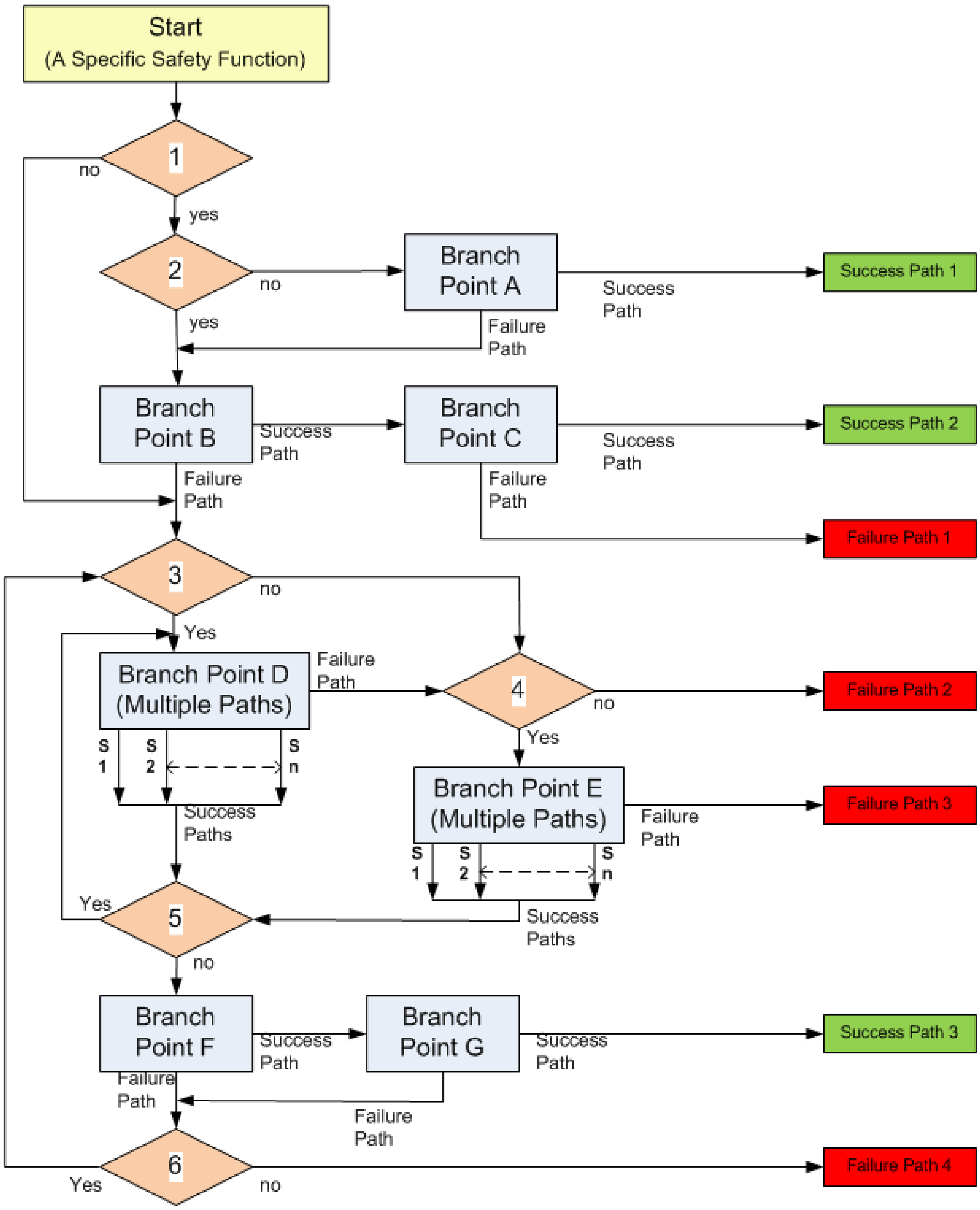


Figure 1. The CRT Flowchart

Table 3. Detailed Description of the Questions in the CRT Flowchart

No.	Question	Description and Example
1	Is the specific function designed to be initiated automatically?	Auxiliary Feed Water is an example of safety function designed to be initiated automatically. Isolation of a steam generator is an example of a safety function that is not designed to be initiated automatically
2	Is the scenario a fast transient?	If loss of Main Feed Water occurs, the Auxiliary Feed Water will be automatically initiated shortly thereafter. Hence, Auxiliary Feed Water is a fast transient
3	Is there a specific entry point to go to the step to manually initiate the safety function?	If there is an entry point in the current procedure to move to another procedure or step to manually initiate the safety function, the answer to this question will be yes. For example, this question

		would refer to the first step to directly transfer from Westinghouse EPG E-0 to the procedure to isolate a steam generator (E-3) if the specific safety function to be analyzed were Steam Generator Isolation.
4	Is there an extra entry point to go to the step to manually initiate the safety function?	If there is an additional entry point in the current procedure to move to (i.e. enter) another procedure or step to manually initiate the safety function, the answer to this question will be yes. Following the Steam Generator Example, all other opportunities to directly transfer from E-0 to E-3 would be identified at this time.
5	Is there another transition point to go to the specific step to manually initiate the safety function or transfer to an incorrect procedure?	If there are any other options in the procedure to lead the operator to manually initiate the safety function, the answer will be yes. Following the Steam Generator Example, all other opportunities to transfer to E-3 will be identified at this time. In other words, any opportunities to transfer from E-0 to E-3 via other procedures will be identified.
6	Are there extra equipment and manual actions that may perform the specific safety function?	If there is any other way to achieve the same result as the safety function, the answer to this question will be yes. This question refers to recovery actions that the crew potentially could take when everything else fails. If there are no opportunities for recovery, the answer will be no.

Table 4. Detailed Description of the Success and Failure Paths for Each Branch Point

BP	**Success Path**	**Failure Path**
A	Operator manually initiate the safety function before it is automatically initiated	Operator does not manually initiate the safety function.
B	The specific safety function is automatically initiated	The specific safety function is not automatically initiated.
C	Operator does not manually turn off the automatically initiated safety function	Operator manually turns off the automatically initiated safety function.
D	An entry point may lead the operator to go to the critical step to manually initiate the safety function. Note that the success paths may be more than one. An entry point may provide multiple choices, and more than one choices may lead the safety function successful. Each successful choice may represent one success path.	Operator chooses the wrong and causes the safety function failed.
E	An entry point may lead the operator to go to the critical step to manually initiate the safety function. Note that the success paths may be more than one. An entry point may provide multiple choices, and more than one choices may lead the safety function successful. Each successful choice may represent one success path	Operator chooses the wrong and causes the safety function failed.
F	The safety function may be manually initiated	The safety function may not be manually initiated (The equipment(s) physically failed and cannot be recovered).
G	Operators successfully initiate the safety function manually	Operators failed to initiate the safety function manually.

4. FAULT TREES, CREW FAILURE MODES, AND PERFORMANCE INFLUENCING FACTORS

A set of fault trees have been proposed to represent a simplified model of human cognition. The trees are developed based on salient information from the cognitive psychology literature in order to bridge the gap between fields of HRA and psychology/human factors. The simplified cognitive model used in these trees has three main parts; Failure in collecting necessary information, Failure in making the correct decision even if necessary information is collected, and Failure in taking the correct action even if the correct decision is made. Table 5 describes the input and output from the Fault Tree exercise.

Table 5. The Input Needed to Apply the Fault Trees and the Output From the Fault Tree Exercise

Input	Output
HFE definition Identified Safety Function Plant context Crew context Developed CRT Identified Critical Paths in the CRT	A list of relevant Crew Failure Modes and Performance Influencing Factors.

Based on the context related to the CRT branch point assessed by the Fault Trees the analyst will trace through the trees. The analyst will eventually encounter an end-point in the trees, which represents the Crew Failure Mode (CFM) associated to the branch point. Examples of CFMs include Information Mis-communicated, Data Not Obtained, Data Discounted, Skip Procedure Step, Deviate From Procedure, Select Wrong Component, and Unintentionally Delay. For the complete set of CFMs, see Figures 2-5 below. The Fault Trees are developed as a template to satisfy all possible scenarios and HFEs. Attempting to satisfy all possible scenarios may result in a large and complex model. To mitigate this and to make the process more practical, the analyst may follow these two principles to simplify the Fault Trees according to the specific context.

1. Determine the property of a specific branch point. For example, if a branch point is to model the operator transmits to a specific procedure, then the information and decision errors are dominant and the action error may be ignored.
2. Determine the status of the flags. If the status of a flag is off, the related fault tree branch may be completely ignored. For example, in a branch point, if the secondary information is not applicable, then “Secondary Information Not Available (Yes=0, No=1)” should be set to 0 and the whole sub-branch of the fault tree may be ignored.

When all relevant CFMs are identified, the analysts will use pre-defined Bayesian Belief Network to identify the Performance Influencing Factors that have the greatest impact for the CFM in the specific critical path or scenario. For example, the CFM Data Discounted in Figure 4 is associated to the PIFs; Knowledge and Experience, Training, Resources (more specifically Procedures), and Human-System Interface. Based on the information gathered during the Scenario Familiarization phase of the analysis, the analyst will assign appropriate relevance to each of the PIFs in the Bayesian Belief Network. The output of the qualitative analysis as a whole is this list of Performance Influencing Factors and their assessed relevance.. This will be handed off to the quantitative part of the HRA, which will calculate the Human Error Probabilities.

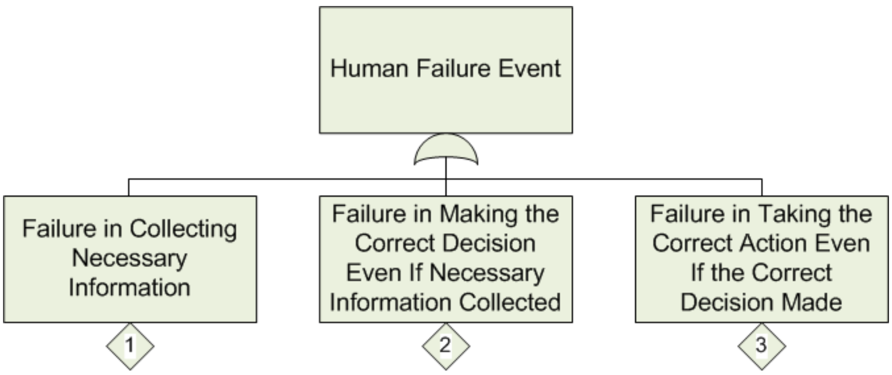


Figure 2. The Top-Level of the Crew Fault Tree

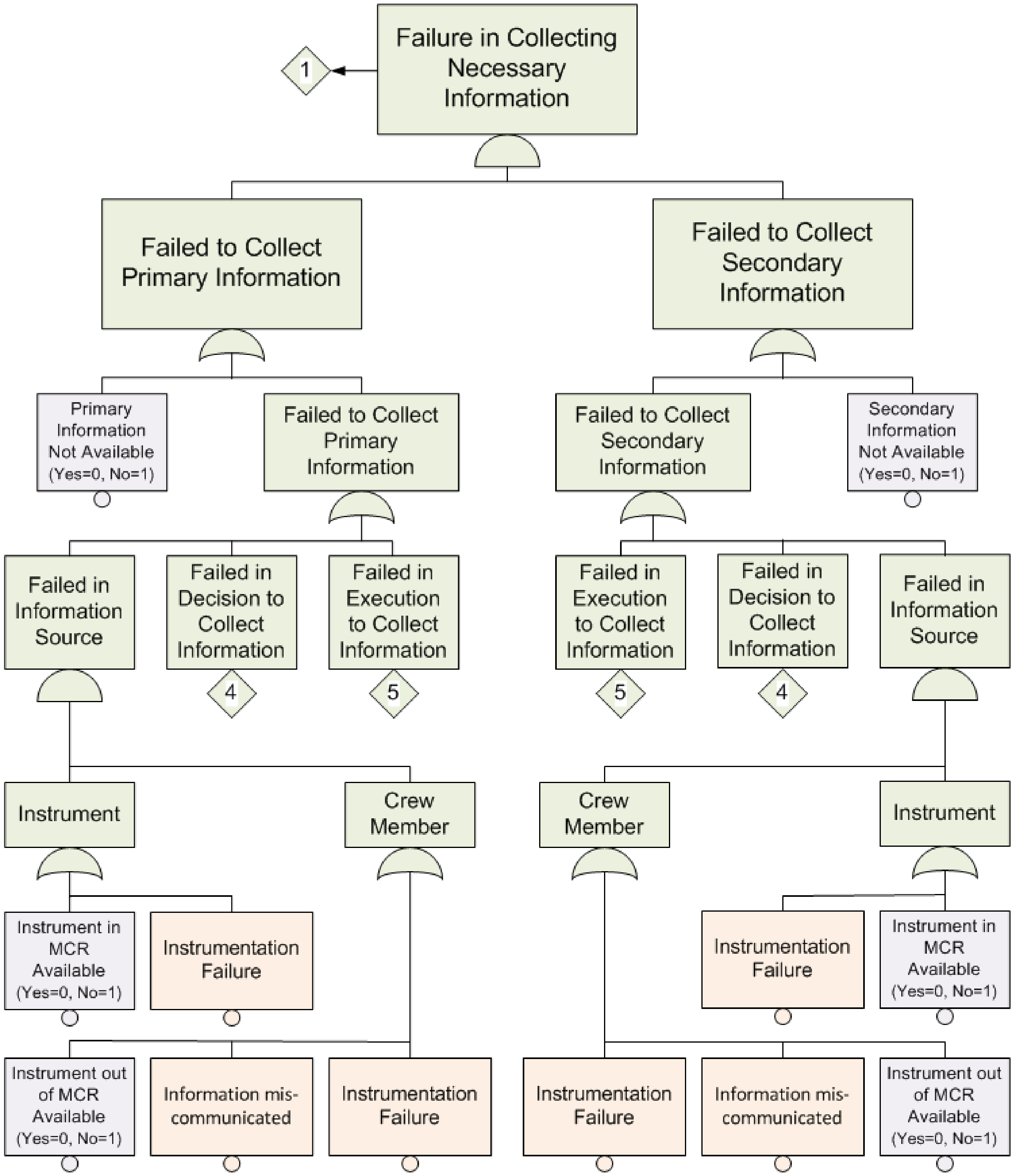


Figure 3. The Failure in Collecting Necessary Information Part of the Fault Tree

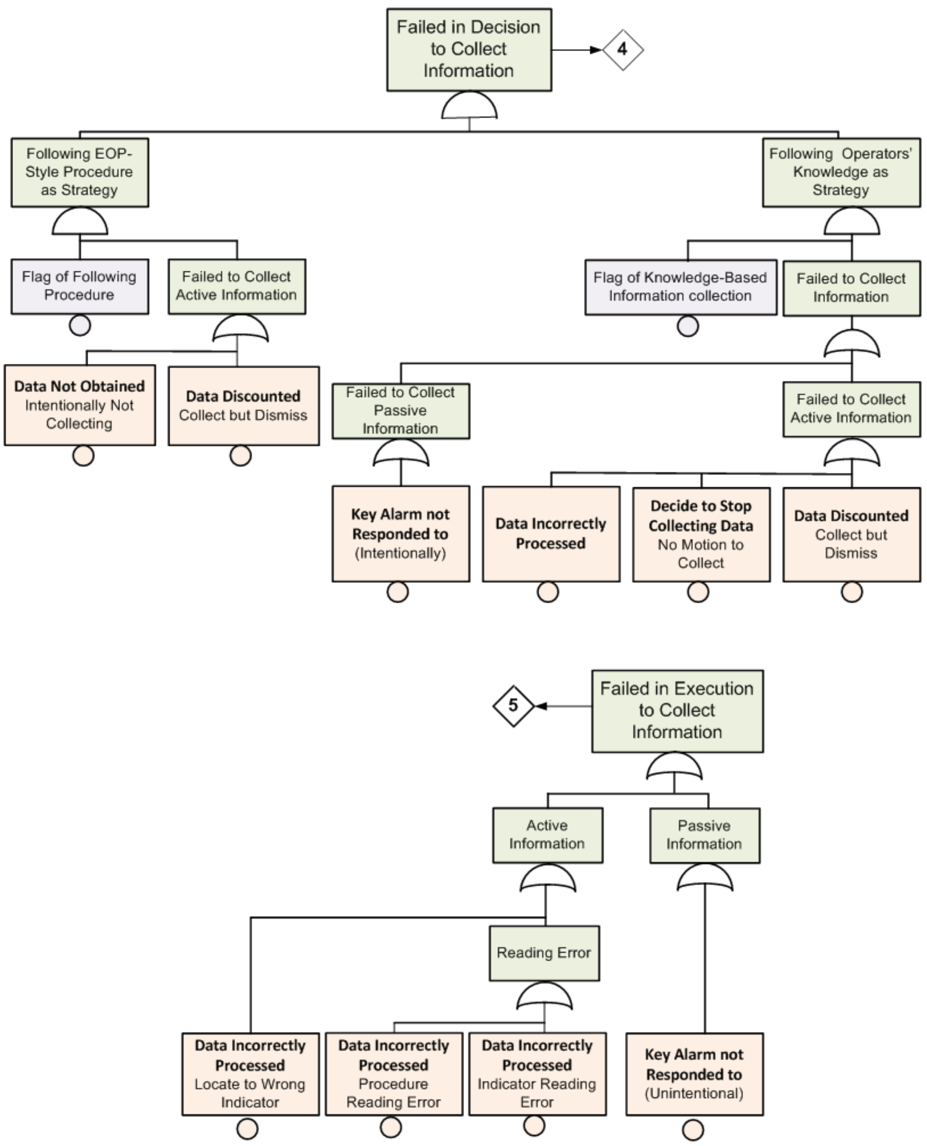
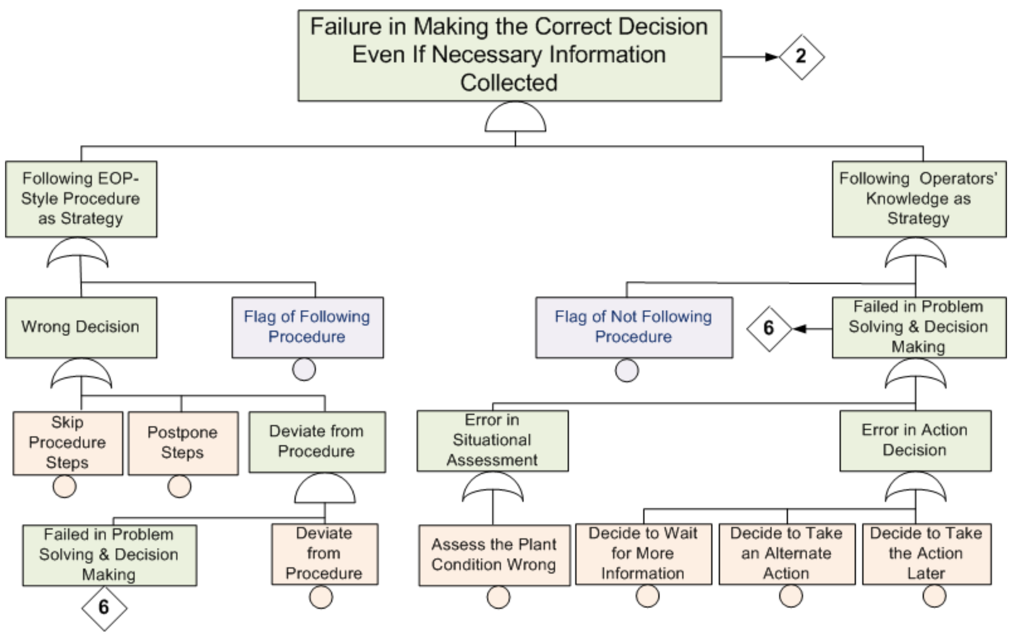


Figure 4. The Failure in Decision to Collect Information and the Failure in Execution to Collect Information Parts of the Fault Tree



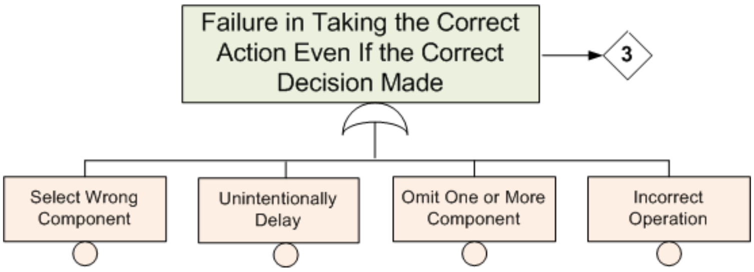


Figure 5. The Failure in Making Correct Decision and Failure to Take Correct Action Parts of the Fault Tree

5. CONCLUSIONS

The main complaints regarding HRA have been that significant analyst-to-analyst variability exists even when the same method is used, that there is a lack of guidance for the qualitative analysis in HRA, and that there is not enough linkage between HRA and Human Factors. The methodology described in this paper attempts to pave the way for removing some of these deficiencies. By using the suggested HRA methodology, the analysts will be able to conduct a qualitative analysis that is detailed and traceable as well as properly documented. The guidance provided is of sufficient detail to be of use for the HRA analysts regardless of their skill levels. The Fault Trees represent a simplified model of human cognition based on salient information from the cognitive psychology literature. The CRT Flowchart and the Fault Trees are tools to help increase the efficiency, reproducibility, traceability, and transparency in the qualitative analysis part of the human reliability assessment. These tools and associated guidance will also help reduce analyst-to-analyst variability within the field of HRA.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the contributions of the late Dr. Dana Kelly to this work.

This work was partially funded by the U.S. Nuclear Regulatory Commission (USNRC) at Idaho National Laboratory (INL) and the University of Maryland. INL is a multi-program laboratory operated by Battelle Energy Alliance for the United States Department of Energy. This work was also supported by the Laboratory Directed Research and Development program at Sandia National Laboratories. Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the US Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. 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.

6. REFERENCES

Mosleh, A., Shen, S-H, Kelly, DL, Oxstrand, J, and Groth, KM (2011). "Model-Based Approach to Human Reliability Analysis: Qualitative Analysis Methodology." *Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM 2012).* Helsinki, Finland

Boring, R. L., Forester, J. A., Bye, A., Dang, V. N., & Lois, E. (2010). *Lessons Learned on Benchmarking from the International HRA Empirical Study*. Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM 2010). Seattle, WA..

Lois, E., Dang, V. N., Forester, J., Broberg, H., Massaiu, S., Hildebrandt, M., et al. (2009). *International HRA Empirical study—Phase 1 Report, Description of Overall Approach and Pilot Phase Results from Comparing HRA methods to Simulator Performance Data*, NUREG/IA-0216, Vol. 1. Washington, DC: US Nuclear Regulatory Commission.

Groth, K. M., Shen, S-H., Oxstrand, J., Mosleh, A., and Kelly, D. (2011). *Model-Based Approach to HRA: Example Application and Quantitative Analysis*. Proceedings of the International Conference on Probabilistic Safety Assessment and Management (PSAM 2012). Helsinki, Finland..