

18 PRA INSIGHTS AFFECTING ESBWR DESIGN

Contents

18.1 INTRODUCTION	18.1-1
18.2 PRA ASSUMPTIONS	18.2-1
18.2.1 Understanding the Effects of Uncertainties on the PRA Model	18.2-1
18.2.2 Identifying Key Assumptions	18.2-1
18.3 INSIGHTS ON THE ESBWR DESIGN	18.3-1
18.4 Maintaining Risk insights and Assumptions.....	18.4-1

List of Tables

Table 18-1 Risk Insights and Assumptions..... 18.4-2
Table 18-2 ESBWR Design Features That Reduce Risk 18.4-7
Table 18-3 Comparison of BWR vs. ESBWR PRA Prevention and Mitigation Functions..18.4-9
Table 18-4 Analysis of Insights and Assumptions (Deleted)..... 18.4-13

List of Figures

Figure 18-1 Process for Identification of Key Insights and Assumptions..... 18.4-12

18 PRA INSIGHTS AFFECTING ESBWR DESIGN

18.1 INTRODUCTION

A comprehensive PRA includes not only the quantified results, but also includes information on how the design features affect the risk profile, and knowledge of the uncertainties, assumptions and limitations of the PRA model in representing an estimate of the risks of the plant. Uncertainty, importance, and sensitivity analyses provide important information about areas where certain design features are the most effective in reducing risk with respect to:

- Operation of reactors;
- Hardware failures and human errors;
- Maintaining the “built-in” plant safety and ensuring that the risk does not increase unacceptably;
- Uncertainty associated with the risk estimates; and
- Sensitivity of risk estimates to uncertainties associated with failure data, assumptions made in the PRA models, lack of modeling details in certain areas, and previously raised issues.

This section describes a systematic approach that is used to define insights and assumptions, identify and evaluate their significance, and to ensure that they are understood and preserved throughout the design phase of the ESBWR.

18.2 PRA ASSUMPTIONS

18.2.1 Understanding the Effects of Uncertainties on the PRA Model

Uncertainty exists in the PRA model where there is no consensus approach or modeling method, and where the choice of approach or modeling method could have an effect on the risk profile such that it influences a risk-based decision made using the PRA. In response to a source of uncertainty, an assumption is created to acknowledge that a best-estimate approach is used, but a different reasonable alternative assumption could produce different results.

During the development phase of the ESBWR, aspects of the design that are not fully complete are treated in the PRA model by using modeling assumptions. As such, it is necessary to identify these assumptions and assure that a process exists to maintain their validity. Different PRA analysts can make different assumptions and still be consistent with the guidelines and standards. The choice of a specific assumption or a particular approximation may, however, influence the results of the PRA. Therefore, it is important to identify significant, or “key,” assumptions and determine if the use of alternative methods or numbers could affect the results and insights of the PRA.

Uncertainties can be categorized into distinct groupings for identification and treatment. Parametric uncertainties are associated with the values of the fundamental parameters of the PRA model, such as equipment failure rates, initiating event frequencies, and human error probabilities. Model uncertainties reflect aspects of the PRA model where the state of knowledge is incomplete because detailed design information is not available during the design phase of the ESBWR, or different options are available for modeling phenomena (for example, different methods for estimating human error probabilities or common cause failures.) Completeness uncertainty, which is an aspect of model uncertainty, reflects areas of the analysis that are not fully developed. This type of uncertainty is typically treated by using conservative, bounding estimates, or by qualitative conclusions that the item is not risk significant and is screened out from further consideration. The effects of uncertainties are assessed by performing quantified analyses or qualitative arguments with conclusions that provide reasonable assurance that, 1) the PRA results represent the as-to-be built plant, and 2) key assumptions are preserved throughout the design phase to ensure they are assessed when making design changes.

18.2.2 Identifying Key Assumptions

An assumption is termed “key” if other reasonable alternatives may exist whose results are significant enough to affect the PRA results and conclusions. A systematic method is used to identify the key assumptions of the PRA model. Sections 1 through 16, and 21 of NEDO-33201 are reviewed to identify instances where parametric, modeling and completeness uncertainties require the use of assumptions. This provides a comprehensive accounting for assumptions from each phase of the PRA development, including the severe accident analysis. Assumptions are identified in each step of the PRA development process. This includes initiating events, accident sequences, success criteria, failure probabilities, human error probabilities, and quantification methods. In addition, each system fault tree logic gate is assessed to identify assumptions that are used, to justify items that are included as well as those that are excluded from the fault tree models. After these assumptions are identified, they are evaluated by a qualitative assessment or sensitivity study to determine their relative significance in terms of the NRC Safety Guidelines

for CDF (<1% change of 1E-4), LRF (<1% change of 1E-6), and CCFP (<0.01 increase). The final result is documentation of all assumptions and a list of key assumptions (i.e., risk significant) and their dispositions, which are as follows:

- Design Requirement: an assumption that requires specific design details be preserved to maintain its validity. Design Requirement key assumptions are controlled by the design organization (GEH).
- Operational Program: an assumption that requires specific operational procedures or training be served to maintain its validity. These key assumptions are implemented in the normal operations phase by the licensees.

18.3 INSIGHTS ON THE ESBWR DESIGN

Insights are considered to be observations or results of the PRA process that should be retained to develop an understanding of its capabilities when applying the model to risk-informed applications. There are insights in the various aspects of the PRA development process. As with assumptions, each earlier section of NEDO-33201 has been reviewed to identify key insights. These insights are also included in Table 18-1.

The advantage of developing the PRA model concurrent with the plant design is in identifying potential risk vulnerabilities and implementing design changes that reduce their risk. In this manner, the risk profile evolves with the design, which lowers the overall risk and reduces dominant risk contributions. The ESBWR PRA has been used extensively during the design phase. Table 18-2 lists design features that contribute to the low core damage frequency and balanced risk profile of the ESBWR. For additional perspective, Table 18-3 provides a comparison of ESBWR vs. BWR design features. Review of the proposed design and use of operating experience has led to significant improvements over currently operating BWR designs in the plant's ability to prevent and mitigate severe accidents. The PRA has already been used to identify and quantify various alternatives for improving the reliability of certain design features found in currently operating BWRs. For example, changing the routing of fire suppression piping reduces the probability of internal flooding, which can disable multiple trains of equipment. Following are examples of PRA-based changes that have been incorporated into the ESBWR design, and consequently have contributed to a significant improvement in nuclear safety:

- (1) Added redundant, physically separated flow paths to the low pressure injection and suppression pool cooling lines in response to fire analysis.
- (2) Determined the loads to be served by the Diverse Protection System, which supplies diverse control signals to safety functions.
- (3) Improved the design of digital controls to reduce the likelihood of inadvertent actuation of specified systems.
- (4) Added redundant supply valves for Isolation Condenser and Passive Containment Cooling pool makeup.
- (5) Added redundant drain line valves for Isolation Condenser System to eliminate a dependency on power supplies.
- (6) Changed the routing of fire suppression piping to reduce the likelihood of room flooding.
- (7) Determined the appropriate locations of control and instrumentation cabinets and power supplies to ensure physical separation.
- (8) Added the Basemat Internal Melt Arrest and coolability device (BiMAC) to reduce the consequences of severe accidents.

18.4 MAINTAINING RISK INSIGHTS AND ASSUMPTIONS

As discussed above, a systematic process is necessary to ensure the continued validity of the model, the following describes the methodology employed.

- (1) Review the NEDO-33201 sections 1 through 16 to identify assumptions and insights.
 - a. Review the section to identify risk insights and assumptions as follows:
 - i. Areas where certain design features are the most effective in reducing risk with respect to operating reactor designs;
 - ii. Major contributors to risk, such as hardware failures and human errors;
 - iii. Major contributors to maintaining the “built-in” plant safety and ensuring that the risk does not increase unacceptably;
 - iv. Major contributors to the uncertainty associated with the risk estimates; and
 - v. Sensitivity of risk estimates to uncertainties associated with failure data, assumptions made in the PRA models, lack of modeling details in certain areas, and previously raised issues.
 - b. Document the identified assumptions.
- (2) Review the system fault tree models, identify and document assumptions for each gate.
- (3) Using the flow chart in Figure 18-1, evaluate key insights and assumptions.
 - a. Determine if evaluation is to be qualitative or quantitative;
 - b. If qualitative evaluation is sufficient, screen against criteria
 - c. If quantitative evaluation required or desired, evaluate against the following criteria:
 - i. CDF/LRF importance measures
 - ii. Sensitivity study cases
 - d. Document results appropriately.
- (4) Document insights and assumptions identified in subject NEDO-33201 sections 1 through 16 and section 21 as follows:
 - a. Summarize all insights and assumptions captured using this process.
 - b. Add to or add a new subsection for “Key Insights” in the subject NEDO-33201 section to capture all key insights and assumptions
- (5) Review insights and assumptions with respect to CDF, LRF, and CCFP.
 - a. Items that are important from a system standpoint, but do not significantly affect CDF, LRF, or CCFP, are retained in system information but are not “key” insights with respect to the DCD application.
 - b. Summarize results in this NEDO 33201 Section (18), Table 18-1.
- (6) Update DCD Tier 2 Chapter 19, Table 19.2-3, with the key insights and assumptions

Table 18-1
Risk Insights and Assumptions

Insight or Assumption	Disposition
Dominant initiating events for internal events: %T-IORV, %T-GEN, %T-FDW, and %T-LOPP are applied using operating experience data. LOCA frequencies (%LL-S-FDWB) are also applied using operating experience data. Overall, none of the dominant initiating events are considered to have unique risk insights.	Insight
The most important Level 2 initiating events are %T-IORV, %T-GEN, and %T-FDW; however, they result in controlled releases. The most important large release initiating event is %LL-S-FDWB, which represents a Large LOCA in Feedwater Line B.	Insight
The containment provides a highly reliable barrier to the release of fission products after a severe accident, with the dominant release category being that defined by Technical Specification leakage (TSL).	Insight
The Level 3 results indicate that the offsite consequences due to internal at-power events are negligible. The results, including sensitivity studies, demonstrate that the estimated offsite consequences are less than the defined individual, societal, and radiation dose limits by several orders of magnitude.	Insight
The ESBWR front-line safety functions are passive and, therefore, have significantly less reliance on the performance of supporting systems or operator actions. In fact, ESBWR does not require operator actions for successful event mitigation until 72 hours after the onset of an accident.	Insight
The ESBWR design reduces the reliance on AC power by using 72-hour batteries for several components. Diesel-driven pumping has been added as a diverse makeup system. The core can be kept covered without any AC sources for the first 72 hours following an initiating fault. This ability significantly reduces the consequences of a loss of preferred (offsite) power initiating fault.	Insight
Anticipated Transients Without Scram (ATWS) events are low contributors to plant core damage frequency (CDF) because of the improved scram function and passive boron injection.	Insight
The ESBWR design reduces the frequency and consequences of loss of coolant accidents (LOCA) due to large diameter piping by removing the recirculation system altogether.	Insight

**Table 18-1
Risk Insights and Assumptions**

Insight or Assumption	Disposition
The design of the ESBWR reduces the possibility of a LOCA outside the containment by designing to the extent practical all piping systems, major system components (pumps and valves), and subsystems connected to the reactor coolant pressure boundary (RCPB) to an ultimate rupture strength at least equal to the full RCPB pressure.	Insight
The probability of a loss of containment heat removal is significantly reduced because the Passive Containment Cooling System is highly reliable due to redundant heat exchangers and totally passive component design.	Insight
The ESBWR is designed to minimize the effects of direct containment heat, ex-vessel steam explosions, and core-concrete interaction The ESBWR containment is designed to a higher ultimate pressure than conventional BWRs.	Insight
Dominant sequences typically do not contain independent component failures. Instead, they consist of common cause failures that disable entire mitigating functions. And, it is important to note that multiple mitigating functions must fail in the dominant sequences, so a single common cause event is insufficient to directly result in core damage.	Insight
The most significant seismic margins contributor is seismic-induced loss of DC power, and ATWS due to seismic-induced failure of the fuel channels and seismic-induced failure of the SLC tank.	Insight
LOCA frequencies. For each pipe group, the number of lines, the number of sections (assessed on the basis of layout drawings), the frequency apportionments, and the final averaged frequencies. These data are binned into the LOCA initiator classes, as summarized in Section 2, Table 2.3-2. Sensitivity study results indicate that changes in the LOCA frequencies have the potential to impact CDF.	Insight
Sensitivity study results indicate that changes in the human error failure probabilities, particularly pre-initiators, have the potential to impact CDF.	Insight
Sensitivity study results indicate that squib valve failure rate estimates have the potential to impact CDF	Insight
Sensitivity study results indicate that changes in test and maintenance unavailability do not significantly impact the CDF or insights.	Insight

Table 18-1
Risk Insights and Assumptions

Insight or Assumption	Disposition
Accident sequences in which DPVs are challenged contribute to approximately 61% of the CDF. In two-thirds of the cases the DPVs are demanded and are successful, and in one-third of the cases the DPVs are demanded and have failed.	Insight
Core damage sequences involving failure of ICS are Class I or III sequences where high pressure makeup has failed and either failure to depressurize occurs or low pressure injection is not available. Given that ICS is failed, the failure of PCCS, or failure to provide make-up to the pools are not significant contributors to core damage frequency.	Insight
FAPCS and FPS injection capability provide adequate core cooling for transients given successful DPV or ADS valve operation, even if containment pressure is at the ultimate containment pressure.	Design Requirement
CRD injection is unaffected by containment overpressurization failure. This is an important assumption, based on the containment failure analysis, that supports the use of CRD in these sequences.	Design Requirement
The DPS cabinet is assumed to be located in a separate fire area in the control building. A preliminary fire PRA analysis model with DPS cabinet located inside room 3301 shows that the fire risk in fire area F3301 would be the dominant contributor to all fire risks due to the high failure probability of common cause failure of software for the safety system, the failure of DPS, and multiple nonsafety-related systems impacted by a fire in room 3301. With a separate fire area for the proposed DPS cabinet in the detailed design, the fire risk can be significantly reduced.	Design Requirement

**Table 18-1
Risk Insights and Assumptions**

Insight or Assumption	Disposition
<p>The ESBWR design features as described in DCD Tier 2 Section 7.1.3 help minimize the adverse affect on safe shutdown due to fire-induced spurious actuations. First of all, the ESBWR instrumentation and control system is digital. A spurious signal cannot be induced by the fire damages in a fiber optic cable. The hard wires are minimized to limit the consequences of a postulated fire. Typically the main control room (MCR) communicates with the safety-related and nonsafety-related DCIS rooms with fiber optics. From the DCIS rooms to the components, fiber optics will also be used up to the Remote Multiplexing Units (RMUs) in the plant. Hard wires then are used to control the subject components. Typically two load drivers are actuated simultaneously in order to actuate the component. To eliminate spurious actuations, these two load drivers are located in different fire areas. Therefore, a fire in a single fire area cannot cause spurious actuation.</p>	<p align="center">Design Requirement</p>
<p>Since the main control room communicates with the DCIS rooms via fiber-optic cables, no spurious actuations due to electrical shorting will be originated from a MCR fire.</p>	<p align="center">Design Requirement</p>
<p>It is assumed that the doors that connect the Control and Reactor Buildings with the Electrical Building galleries are watertight, for flooding of the galleries up to the ground level elevation.</p>	<p align="center">Design Requirement</p>
<p>The Class IV (ATWS) sequences experience core damage at high pressure because ADS is inhibited as part of the core damage mitigation effort. However, it is assumed that Emergency Operating Procedures (EOPs) will instruct the operator to depressurize after core damage has occurred in an attempt to preserve containment. It is shown in Appendix 8A that the frequency of ATWS sequences experiencing RPV rupture at high pressure is negligible, so only failures at low pressure were analyzed.</p>	<p align="center">Operational Program</p>
<p>Venting is assumed to occur when the containment pressure reaches 90% of the ultimate containment strength.</p>	<p align="center">Operational Program</p>
<p>During shutdown conditions, a fire barrier may not be intact due to maintenance activities. However, an added fire watch would not only increase the success probability of fire detection and suppression, but also help restore the fire barrier in time to prevent fire propagation. Shutdown fire risks related to the fire barriers are evaluated and managed in accordance with the outage risk management program of 10CFR50.65(a)(4).</p>	<p align="center">Operational Program</p>

**Table 18-1
Risk Insights and Assumptions**

Insight or Assumption	Disposition
All LOCAs below TAF during shutdown require closure of lower drywell hatch. The hatch can be opened during shutdown. If a break occurs in the lower drywell and the hatch is not closed, core damage is assumed to occur (once the water level reaches the bottom of the hatch, it is assumed that the door can not be closed and the leak not isolated).	Operational Program
An important recovery action during shutdown is to recover at least one train after loss of both operating RWCU/SDCS trains.	Operational Program
An important recovery action during shutdown is to recover Service Water function after loss of PSW.	Operational Program
The plant should not be in a Mode 6 Unflooded condition when a hurricane strike occurs. This is because in Mode 6 unflooded the containment is open, the reactor vessel is open and the water above the core will not keep the core cool for an extended period of time.	Operational Program
The greatest contribution to shutdown risk comes from breaks in lines connected to the vessel below TAF. In these cases, the lower drywell equipment hatch or personnel hatch is likely to be open to facilitate work in the lower drywell. Although the frequency of these events is very low, there is only one method for mitigation – manual closure of the hatch(es).	Operational Program
The dominant risk contributor with respect to shutdown modes is “Mode 6 Unflooded.” This is consistent with the baseline shutdown CDF results since the isolation condenser system is not credited in the Mode 6 Unflooded event trees. Therefore, it is necessary to ensure the operability of the systems critical to decay heat removal function during this mode.	Operational Program
It is assumed that the watertight doors are normally closed at power. Opening of the doors would generate an alarm in the Control Room, and procedures direct their immediate closure upon receipt of an alarm.	Operational Program
It is assumed that, during shutdown, manual and automatic depressurization (ADS) of the vessel are available while the vessel head is in place.	Operational Program
It is assumed that the actuation of the GDCS due to an RPV Level 1 water level signal is available during the entire shutdown period.	Operational Program

Table 18-2
ESBWR Design Features That Reduce Risk

<p>Reactor Vessel</p> <p>Increased volume of water in vessel</p> <p>No recirculation pump headers minimizes Large Loss-of-Coolant-Accident potential</p> <p>Smaller diameter piping connected to vessel below core elevation</p>
<p>Isolation Condenser System</p> <p>Redundant and Diverse active components</p> <p>Cooling Pools vs. shell-side heat exchangers</p> <p>In-line condensate reservoirs</p>
<p>Gravity Driven Cooling System</p> <p>Eliminate reliance on pumps and motor-operated valves</p>
<p>Passive Containment Cooling System</p> <p>No active components</p> <p>Independent of AC Power to operate</p>
<p>Standby Liquid Control System</p> <p>Two pressurized tanks of sodium pentaborate</p> <p>No pumps required for injection to vessel</p>
<p>Reactor Water Cleanup/Shutdown Cooling</p> <p>Uses larger heat exchangers for backup decay heat removal</p> <p>Full pressure shutdown cooling capability</p>
<p>Fuel and Auxiliary Pool Cooling System</p> <p>Low Pressure Coolant Injection mode for backup coolant injection</p> <p>Automatic Suppression Pool Cooling mode</p>
<p>Control Rod Drive System</p> <p>Provides high pressure injection to vessel</p>

Table 18-2
ESBWR Design Features That Reduce Risk

<p>ATWS Prevention/Mitigation</p> <p>Scram Discharge Volume eliminated</p> <p>Fine Motion Control Rod Drives provide diverse backup</p> <p>Automatic, safety-related Standby Liquid Control System</p> <p>Alternate Rod Insertion</p>
<p>Instrumentation and Control</p> <p>Multiple diverse systems to minimize common cause failures</p>
<p>Severe Accident Mitigation</p> <p>BiMAC device added to eliminate the uncertainty of ex-vessel debris coolability and core-concrete interaction gas generation</p> <p>Fire water injection capable of arresting core melt in-vessel (not modeled in PSA)</p> <p>Inert containment prevents hydrogen combustion</p> <p>High ultimate rupture strength of containment</p>
<p>Loss of Preferred Power</p> <p>Plant capable of "island mode" of operation in the event of loss of grid (not modeled in PSA)</p>

**Table 18-3
Comparison of BWR vs. ESBWR PRA Prevention and Mitigation Functions**

Prevention or Mitigation Function	BWR Features	ESBWR Features	Net Effect of ESBWR Design and Operation Features
Initiating Events - Transients	Turbine Trip, Loss of Offsite Power, Loss of FW	Turbine Trip, Loss of Offsite Power, Loss of FW	Similar
Initiating Events – LOCAs, Line Breaks Outside Cont., ISLOCA, Reactor Vessel Rupture	Small, Medium, Large LOCA, LBOC, ISLOCA, Vessel Rupture	Small, Medium, Large LOCA, LBOC, ISLOCA, Vessel Rupture	ESBWR has significantly less large bore piping outside of vessel due to elimination of Recirculation Pumps. Large LOCA and ISLOCA frequencies are lower. ESBWR high to low pressure interfaces use piping capable of withstanding vessel rupture pressure – reduces Interfacing Systems LOCAs.
Reactivity Control	RPS ARI RPT SLC ATWS RPV Level Control	RPS ARI FW Runback SLC ATWS RPV Level Control	Similar Similar ESBWR FW Runback performs similar function to BWR RPT. BWR SLC requires AC Power, ESBWR SLC is accumulator-driven and does not require AC Power to initiate. Level Control treated similarly. ESBWR ADS Inhibit function is automatic.

**Table 18-3
Comparison of BWR vs. ESBWR PRA Prevention and Mitigation Functions**

Prevention or Mitigation Function	BWR Features	ESBWR Features	Net Effect of ESBWR Design and Operation Features
High Pressure Mitigation	HPCS/ HPCI RCIC CRD 2-Division Analog Actuation	Isolation Condenser CRD 4-Division Digital Actuation	ESBWR does not have a high pressure coolant injection pump. CRD pump capacity and discharge head are enhanced in ESBWR to provide high pressure injection capability. ESBWR uses Isolation Condenser to mitigate transients and prevent need to depressurize. Isolation Condenser does not require AC or DC power, or operator action to control vessel level by controlling pump flow.
Depressurization	Manual SRVs Automatic ADS SRVs	Manual SRVs Automatic ADS SRVs ADS DPVs	ESBWR uses SRVs and DPVs. DPVs are squib-actuated and do not reclose. ESBWR uses manual depressurization with SRVs to preclude the need for ADS. No re-pressurization with DPVs
Low Pressure Mitigation	LPCS LPCI Fire Water Injection	GDCS Injection GDCS Equalize FAPCS LPCI Fire Water Injection	Both GDCS subsystems are independent of AC or DC power. FAPCS LPCI function provides injection with in-line heat exchanger.

**Table 18-3
Comparison of BWR vs. ESBWR PRA Prevention and Mitigation Functions**

Prevention or Mitigation Function	BWR Features	ESBWR Features	Net Effect of ESBWR Design and Operation Features
Containment Heat Removal	RHR Heat Exchangers Venting	PCCS FAPCS Supp. Pool Cooling RWCU SDC Venting	PCCS is independent of AC or DC power. RWCU SDC provides high pressure cooling.
Supporting Functions	AC Distribution Diesel Generators DC Distribution Component Cooling Room Cooling	AC Distribution Diesel Generators DC Distribution Component Cooling Room Cooling	ESBWR Passive Safety-Related Systems require no Supporting Functions for 72 hours. ESBWR DC System uses 72 hour capacity batteries for safety-related functions. BWR vs. ESBWR component and room cooling are similar.
Instrumentation and Control Systems	Analog single-failure proof. Digital in limited use (FW level controller in some plants.)	Digital Controls. Diverse Protection System.	Digital Controls with triple-redundancy. Diverse Control for key functions to eliminate the effects on common-cause failures, e.g., software.
Severe Accident Mitigation	Severe Accident Guidelines	Severe Accident Guidelines BiMAC	BiMAC reduces the containment failure probability from core-concrete interaction.

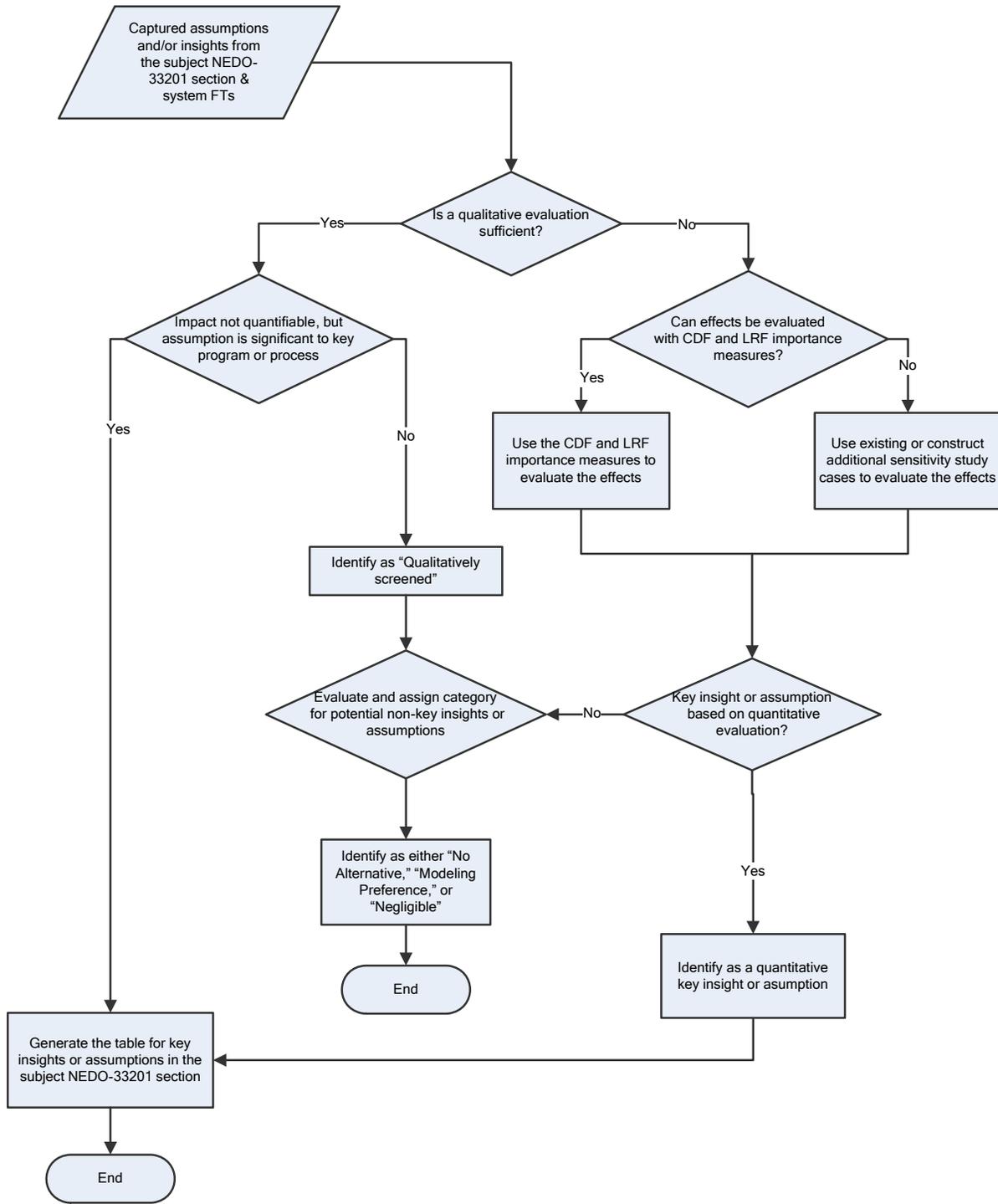


Figure 18-1 Process for Identification of Key Insights and Assumptions

Table 18-4

Analysis of Insights and Assumptions (Deleted)