Risk Assessment of Operational Events

Handbook

Volume 3 – SPAR Model Reviews

Review Checklists – Key Assumptions and Technical Issues
Bibliography

Revision 2

September 2010

SDP Phase 3 ● ASP ● MD 8.3

TABLE OF CONTENTS

LIST OF TABLES

ACRONYMS

ac	alternating current
ADS	automatic depressurization system
ASME	American Society of Mechanical Engineers
ASP	accident sequence precursor
BWR	boiling water reactor
CDP	core damage probability
CCCG	common cause component group
CCF	common-cause failure
dc	direct current
EDG	emergency diesel generator
EPIX	Equipment Performance and Information Exchange
FSAR	Final Safety Analysis Report
HEP	human error probability
HPCI	high-pressure core injection
HRA	human reliability analysis
LER	licensee event report
LOCA	loss-of-coolant accident
LOOP	loss of offsite power
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PWR	pressurized water reactor
RCIC	reactor core isolation cooling

SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SDP	Significance Determination Process
SPAR (model)	Standardized Plant Analysis Risk (model)
SRA	Senior Reactor Analyst
SRV	safety relief valve
SSC	structure, system, and/or component
T/M	test and maintenance
TS	Technical Specifications

SPAR Model Reviews: Introduction	Section 1
	Rev. 2

1.0 Introduction

1.1 Objectives

The main objective of these checklists are to ensure that the SPAR models used in the risk analysis of operational events represent the as-built, as-operated plant to the extent needed to support these analyses. Specifically, the specific objectives are as follows:

☐ ***Model completeness.*** To check whether the SPAR model reflects the as-built, as-operated plant for the important sequences that are impacted by the operational event under consideration; to check that the SPAR model reflects the plant features required to model the operational event and/or to replace overly conservative model assumptions with best available information on more realistic assumptions.

☐ ***Key Assumptions.*** To check whether the key assumptions in a SPAR model are adequately considered in the logic model for important sequences that are impacted by the operational event.

☐ ***Key issues.*** To check that key technical issues have been addressed in the SPAR model for important sequences that are impacted by the operational event under consideration, and associated limitations have been identified by the use of sensitivity and uncertainty studies.

☐ ***Success criteria.*** To check the success criteria of the frontline systems under the specific boundary conditions of each initiator group.

☐ ***Event trees.*** To check whether the plant response to accident initiators is adequately modeled by the functional and systemic event trees; to identify systems whose functioning or recovery times are dependent upon the previous state of other systems.

☐ ***Fault trees.*** To check whether the fault trees adequately represent the frontline systems as far as their failure modes are concerned and the identified dependencies are correctly reflected in the fault trees.

☐ ***Parameter estimations.*** To check the assessment of point values and corresponding uncertainties for the parameters necessary for the quantification of accident sequences.

☐ ***Recovery modeling.*** To check the modeling of system recovery.

☐ ***Model solution.*** To review inputs and modifications to the SPAR model; to review model solution (quantification) results.

☐ ***Assumptions and issues.*** To summarize the key SPAR model assumptions and technical issues.

1.2 Use of Checklists

The appropriate checklists should be used following modifications to SPAR models that are used to perform risk analysis of operational events in conjunction with the Significance Determination Process (SDP) Phase 3, NRC Incident Investigation Program (Management Directive 8.3), and Accident Sequence Precursor (ASP) Program.

It is expected that all but the simplest modifications to SPAR models will be performed by the SPAR model developer or a probabilistic risk assessment (PRA) practitioner at the advanced level. In such cases, the SPAR model developer or practitioner should perform the necessary review following each modification to the SPAR model.

In the cases where simple, routine modifications are made by Regional Senior Reactor Analysts (SRAs) and other risk analysts, the responsible analyst should ensure that such modifications were proper and complete. These checklists provide guidance for the analyst to help in the review process.

In all cases, the analyst should ensure that the SPAR model represents the as-built, as-operated plant to the extent needed to support the event-specific analysis. The responsible analyst should ensure that applicable changes to the as-built, as-operated plant are properly reflected in the SPAR model.

1.3 About Checklists

The checklists provided in Section 2.0 in this volume of the handbook represents best practices based on feedback from experience in risk analysis of operational events. Since PRA methodologies, as well as the tools and models used in the risk analysis of operational events are continually changing, such lists would be revised when some practices become out of date.

The checklists presented in Section 2.0 are based on the following documents:

- PRA Review Manual, NUREG/CR-3485, 1985

- "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-informed Activities," Regulatory Guide 1.200, January 2007

- NRC Regulatory Position on ASME PRA Standard ASME RA-S-2005, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," 2005

- ASP Program review checklist

- SPAR Model Development Program checklists

- Lessons learned from the reviews of ASP and SDP Phase 3 analyses

Where appropriate, the checklist items are cross-referenced with the applicable ASME standard index number(s). Given that most analysis activities involving SPAR models are related to modifications to an existing model and not related to development of a PRA from scratch, not all requirements in the ASME standard are represented in these checklists. In addition, suggested review items for ensuring the proper uses of the SPAR model and SAPHIRE/GEM code are included.

Lastly, it is assumed that these checklists are designed for an analyst involved with SPAR model modifications who has advanced experience in PRA modeling.

> *"Remember, if your system passes all the following checklists, it merely proves that it has passed the checklists.*
>
> *Completed checklists should not be taken as the sole evidence that you have a good system. They are rather like intelligence test - these tend to show how good you are at passing intelligence tests, not how intelligent you really are! At the end of the day your users will tell you if the system is any good."*
>
> ORACLE (1990)

1.4 About SPAR Model Assumptions and Issues

Section 3 of this Handbook volume summarizes key assumptions in a SPAR model and unresolved technical issues that may produce large uncertainties in the analysis results. The importance of these assumptions or issues depends on the sequences and cut sets that were

impacted by the operational event. Additionally, plant-specific assumptions and issues may play an even larger role in the analysis uncertainties.

The list of key assumptions and issues in Section 3 represents a current perspective, since PRA technology and experience are constantly used to improve PRA models. Therefore, the analyst is advised to periodically review up-to-date information on SPAR model assumptions and technical issues. Information resources include the following:

- ***Plant-specific assumptions and issues.*** Key assumptions in a plant-specific SPAR model are documented in the plant SPAR model manual. A summary of the information in a SPAR model manual is provided in Table 1.

In particular, Appendix F of the plant SPAR manual, "Disposition of Comments from Site Visits," summarizes benchmarking results and differences between SPAR and the licensee's PRA model.

- ***Generic technical issues.*** The status of generic technical issues that apply to most SPAR models can be viewed from the SAPHIRE User Group Web site. These issues represent the major differences between SPAR models and licensee PRA models that were identified in site visits during SPAR model development and the benchmarking effort of the Mitigating System Performance Indicator (MSPI) project. The SPAR model development program is actively engaged in resolving issues involving large uncertainties.

- ***Pending plant-specific modifications***. A plant model may have a list of pending modifications that will be incorporated in the next model revision. These future modifications include potential global errors identified from other models, enhancements made during previous analysis, and resolution of generic technical issues. A listing of pending plant-specific modifications can be found in the SPAR model file, and can be viewed from the SAPHIRE User Group Web site.

1.5 Technical Contacts

Comments and/or corrections are appreciated. Comments should be directed to the following:

- Volume 1, Internal Events – Don Marksberry, 301-415-6378, dgm2@nrc.gov
- Volume 2, External Events – Selim Sancaktar, 301-415-8184, sxs9@nrc.gov
- Volume 3, SPAR Model Reviews – Peter Appignani, 301-415-6857, pla@nrc.gov

Table 1. Summary of the information in a plant-specific SPAR model manual.

Sect	Section Topic	Useful Information
	Notes to Analysts	• Truncation • Use of template events • Global data changes
1	Introduction	
2	Initiating Events Data	• Basis for the identification and quantification of initiating events • Table - Initiating event frequencies and uncertainty data
3	Event Tree Models	• Event tree assumptions • Event tree descriptions and figures • Table - Success criteria • Table - SAPHIRE sequence flag sets • Table - SAPHIRE event tree linkage rule
4	Fault Tree Models	• Fault tree assumptions • Fault tree descriptions • Table - Fault tree flag sets
5	Basic Event Data	• Template and compound event descriptions • Table - template event data
6	Common Cause Failure (CCF) Model	• CCF model description
7PWR	Reactor Coolant Pump (RCP) Seal Loss-of-Coolant Accident (LOCA) Model (PWR)	• RCP seal LOCA model description

Sect	Section Topic	Useful Information
8PWR 7BWR	Loss of Offsite Power (LOOP) Model	• LOOP model description • Table - LOOP frequency parameters • Table - LOOP non-recovery parameters • Table - Emergency diesel generator repair probabilities • Figure - LOOP non-recovery probabilities
9PWR 8BWR	Human Reliability Model	• Human reliability model description • Table - Human action data • Table - Dependent human actions • Listing - SAPHIRE project recovery rules (maintenance combinations, system alignment rules, human error probability dependency rules)
10PWR 9BWR	Baseline Results	• Table - Initiating event contribution to overall core damage probability • Table - Baseline core damage risk results • Table - Baseline importance measure results
App A	Fault Trees	Table - Fault tree to event tree list
App B	Basic Event Data Report	Table - Basic event data with source references
App C	Compound Event Data Report	Table - Compound event data
App D	Common Cause Failure Event Data Report	Table - CCF event data
App E	SPAR Human Reliability Analysis (HRA) Event Data Report	Table - HRA event data with performance shaping factor levels
App F	Disposition of Comments from Site Visits	• Table F-1: Summary of benchmarking results • Table F-2: Differences between SPAR and the licensee's PRA
App G	Simplified Diagrams	Simplified online diagrams for select electrical and mechanical systems

SPAR Model Reviews: Review Checklists	Section 2
	Rev. 2

2.0 Review Checklists

2.1 As-Built, As-Operated Plant Description

Objectives

The main objectives of this part of the review are the following:

☐ To check whether the SPAR model reflects the as-built, as-operated plant for the important sequences that are impacted by the operational event under consideration.

☐ To check that the SPAR model reflects the plant features required to model the operational event and/or to replace overly conservative model assumptions with best available information on more realistic assumptions.

These checks should be performed on the base case (baseline) and current case of the SPAR model. The checklist items are cross-referenced with the applicable ASME standard (Ref. 4.7-1) index number(s).

Review Checklist

☐ ***SPAR model revision.***

- o *SPAR model.* Check the SAPHIRE User Group Web site to ensure that the original baseline SPAR model is of the most up-to-date revision.

- o *SAPHIRE/GEM.* Check the SAPHIRE User Group Web site to ensure that the SAPHIRE/GEM code is of the most up-to-date release or the desired release of the code.

SPAR NOTE: The use of a different release of SAPHIRE may generate slightly different results. These results may differ from the baseline results documented in the plant-specific SPAR model manual.

- o *Documentation.* Check that the plant-specific SPAR model manual reflects the model downloaded from the Idaho National Laboratory (INL) server. Run the original baseline model (before modifications of the baseline model) from the server and compare the results with the documentation.

☐ ***Plant/procedure modifications.*** Check for recent plant and procedure modifications associated with important sequences. However, only those modifications that existed at the time of the operational events should be considered in the analysis.

☐ ***System interactions.*** Check that observed or relevant potential component/system interactions are addressed in the model. (e.g., water deluge from inadvertent actuation of fire protection sprinkler system causing damage to nearby electrical equipment).

☐ ***Plant status.*** Check that observed plant operating status (e.g., at-power operations vs. shutdown operations), including relevant support system status (e.g., available, inoperable, etc.), are addressed in the model.

☐ ***System/train configurations.*** The following checks should be performed using plant layout diagrams, system piping and instrumentation diagrams, and simplified electrical and system line diagrams.

- o *Impacted systems.* Check that systems are configured to represent the plant status at the time of the event.

- o *Standby and swing components.* Check that available standby and swing components are configured to represent the plant status at the time of the event.

- o *Atypical configurations.* Check that relevant atypical configurations of trains/components are configured to represent the plant status at the time of the event.

  Examples of atypical configurations include pressurizer power-operated relief valve (PORV) block valves in the closed position during power operations and electrical power distribution during maintenance.

- o If not, check that the modeled system configuration will not significantly impact the results of the assessment. Sensitivity analyses may be used to check the importance of system configurations.

☐ ***Operator actions.*** Check that relevant operator actions are addressed in the model. Relevant operator actions should be revised against appropriate normal, abnormal, and emergency operating procedures.

☐ ***Alternative mitigating strategy.*** Check the basis for crediting a newly added mitigating strategy or system. This check should include the following:

- ○ *Engineering analysis or system testing* has shown that the mitigating strategy would be successful throughout the accident scenario.
- ○ *Operating procedures* for using the strategy existed at the time of the operational event occurrence.
- ○ *Operator training* for implementing the strategy existed at the time of the operational event occurrence.
- ○ *Environmental conditions* allow feasible implementation of alternative strategy to cope throughout the accident scenario.
- ○ *Support systems and instrumentation* would be available to support the alternative strategy throughout the accident scenario.

The mitigating strategy may involve safety and/or non-safety related systems.

☐ ***Future changes.*** Check whether pending changes to the SPAR model (in the queue for plant model revision by the SPAR model developer) that are relevant to the operational event are included in the revised baseline model.

☐ ***Previous model uses.*** If available, review one-time modeling changes made in previous SDP and ASP analyses for applicability to the event. Ask the previous analyst about relevant modeling issues.

☐ ***Model simplifications.*** Check for relevant SPAR model simplifications, such as

- o Undeveloped event tree transfers.
- o Event trees that model only one support system train (e.g., loss of dc).
- o Historical basic event values for rare events.
- o Phantom or inactive basic events which values are set to “IGNORE” or “TRUE” in the base case SPAR model. Such basic events may be undeveloped events or may have been events created exclusively for past analyses.

2.2 SPAR Model Assumptions and Technical Issues

Objectives

The main objectives of this part of the review are:

- To check whether the key assumptions in a SPAR model are adequately considered in the logic model for important sequences that are impacted by the operational event.

- To check that key technical issues have been addressed in the SPAR model for important sequences that are impacted by the operational event under consideration, and associated limitations have been identified by the use of sensitivity and uncertainty studies.

The checklist items are cross-referenced with the applicable ASME standard (Ref. 4.7-1) index number(s).

Review Checklist

☐ ***Usage limitations screen.*** Read and understand the Usage Limitations screen on SAPHIRE/GEM for the plant-specific SPAR model.

☐ ***SPAR model vs. PRA.*** Read the Acceptance Criteria, found in the "DOC" folder in the SPAR model file, to better understand key differences between the SPAR model and licensee's PRA.

☐ ***Key SPAR model assumptions.*** Check that relevant key SPAR model assumptions associated with important sequences, and structures, systems, and components (SSC) failure modes were identified and addressed in the analysis (e.g., model modification, engineering assumptions, etc.).

Modeling assumptions used in SPAR models are documented in the plant-specific SPAR model manual. Key generic assumptions are summarized in Section 3 of this Handbook volume.

☐ ***Key generic technical issues.*** Check that relevant key technical issues associated with important sequences and SSC failure modes were identified and addressed in the analysis (e.g., model modification, engineering assumptions, etc.).

Generic technical issues affecting SPAR model logic are summarized in Section 3 of this Handbook volume.

☐ ***Pending plant-specific modifications.*** Check that pending plant-specific modifications associated with important sequences and SSC failure modes were identified and addressed in the analysis (e.g., model modification, engineering assumptions, etc.). These pending modifications are typically waiting to be incorporated in the next revision of the model by the SPAR model developer.

The list of pending modifications for each plant model can be downloaded from the SAPHIRE User's Web site.

☐ ***Sensitivity analyses***. Check whether key assumptions in the SPAR model and technical issues associated with important sequences and SSC failure modes have been addressed in sensitivity analyses.

2.3 Success Criteria

Objective

The objective of this part of the review is to check the success criteria of the frontline systems under specific boundary conditions of each initiator group. This provides background information for more detailed checking of the success criteria in the review of event trees and fault trees in a SPAR model.

The checklist items are cross-referenced with the applicable ASME standard (Ref. 4.7-1) index number(s).

Review Checklist

☐ ***Core damage definition.*** Check the definition of core damage (e.g., fuel melting, cladding degradation, core uncovery) and assumptions used to determine the success criteria (e.g., peak cladding temperature for core damage). (SC-A2)

☐ ***Mitigating functions.***

- o *Minimum set of functions.* Check the minimum set of mitigative functions to prevent core damage in the accident sequences. (SC-A3)

- o *Success criteria.* Check the success criteria for each mitigating function were appropriately defined. (SC-A4)

- o *Basis.* Check the basis for establishing the success criteria of the mitigating function, e.g., Final Safety Analysis Report (FSAR) transient analysis; best-estimate, plant-specific transient analysis; best-estimate, generic transient analysis; expert judgment. (SC-B1)

- o *Conservative assumptions.* Check for any apparent conservative or optimistic assumptions in the success criteria analysis, especially, conservatism in an FSAR analysis.

- o *Technical reviews.* Check whether a knowledgeable specialist reviewed the reasonableness and acceptability of the results of the thermal hydraulic, structural, or other supporting engineering bases that were used to justify the success criteria. (SC-B5)

☐ ***Mitigating systems.***

- o *Success criteria.* Check the systems capable of meeting the specified mitigating function success criteria. (SC-A4)

- o *Shared systems.* Check the mitigating systems that are shared between units, and the manner in which the sharing is performed should both units' experience a common initiating event (e.g., dual unit LOOP, loss of a shared support system). (SC-A4)

☐ ***Alternative mitigating strategies.*** Check the basis of an alternative mitigating strategy. Refer to "Alternative mitigating strategy" in Section 2.1 for criteria for crediting a new strategy.

☐ ***System restarts.*** Check the assumptions that justify the requirement of the restart of specific systems.

☐ ***Manual initiations.*** Check the time available for manual initiation of systems when auto-initiation fails.

☐ ***Mission times.***

- ○ Check the mission time for each frontline system. (SC-A5)

- ○ Note: Mission times are typically closely coupled with its success criteria. The

success criteria for a system can be event and sequence dependent. Any changes to the mission time of a system should reflect the sequence success criteria of that system.

☐ ***Comparing results.***

- o *SPAR manual.* Check that the success criteria defined in the plant-specific SPAR model manual was consistently used in the event tree.

- o *Plant PRA.* Compare the success criteria with those from the plant PRA (via reviews, if available). Check the validity of similarities, and account for differences.

2.4 Event Trees

Objectives

The main objectives of the event tree review are the following:

- To check whether the plant response to accident initiators is adequately modeled by the functional and systemic event trees.

- To identify systems whose functioning or recovery times are dependent upon the previous state of other systems.

The checklist items are cross-referenced with the applicable ASME standard (Ref. 4.7-1) index number(s).

Review Checklist

☐ ***Top events.*** Check that top events represent the key safety functions that are necessary to prevent core damage, and reach a stable state. (AS-A2)

Top events include the following:

- o Systems that can be used to mitigate the initiator for each key safety function. (AS-A3)
- o Procedurally directed operator actions for each key safety function. (AS-A4)

☐ ***Logical order of top events.*** Check the logical ordering of top events as they are required subsequent to the onset of the initiating event. (AS-A6)

☐ ***Dependencies of top events.***

- o *Initiator impacts.* Check for systems which are immediately disabled or degraded by the initiating event. (AS-B1)

- o *Accident progression.* Check for systems which are either disabled or degraded by phenomenological conditions created by the accident progression. Phenomenological impacts include generation of harsh environments affecting temperature, pressure, debris, water levels, and humidity. (AS-B3)

- o *Initiator to system dependency.* Check the dependencies between initiating event and those systems or functions which are required at a later time (i.e., a function's dependence on the success or failure of preceding functions). (AS-B2)

- o *System to system dependency.* Check the functional dependency between systems, (e.g., failure of one system resulting in another system failure to perform its function successfully). (AS-B2)

- o *Support system to frontline system dependency.* Check for dependencies between support systems and frontline safety systems. (SY-B5)

- o *Basis.* Check the thermal hydraulics analysis assumptions used to support the bases of the dependency or lack thereof. (AS-A9)

☐ ***Success criteria of top events.***

- o See the checklist for success criteria.

☐ ***Event tree linking rule.*** If multiple fault trees are required for different sequences, check the event tree linking rule that links the correct fault tree to the specific sequence.

☐ ***Recovery modeling.***

- o *Event tree level.* Check for system recovery in the event tree as the top event.

- *Fault tree level.* If system recovery is not modeled in the event tree, then check the recovery model in the fault tree(s).

- *Cut set level.* If system recovery is considered on a cut set basis, then check the recovery model in the project recovery rules.

☐ ***Operator actions.*** (AS-A4)

- *Procedures.* Check that operator actions included in the event trees are consistent with plant procedures.

- *Logical order.* Check that the logical ordering of top events representing operator errors is consistent with

  – Respective times within which the actions must be performed.
  – Indications available to the operator which affect the success of the action.

☐ ***Transfer trees.*** (AS-A11)

- Check that important “transfers” between trees (i.e., accident sequences that initiates a different accident sequence), are complete and properly modeled.

- Check for transfers of sequences to other event trees because of additional failures, (e.g., transient-induced LOCAs or stuck-open safety relief valve (SRV) or PORV, transient- or LOCAs-induced loss of offsite power).

☐ ***Sequence damage states.*** (AS-A8)

- *Core damage definition.* Check for consistent definition of core damage (e.g., core uncovery is used in SPAR models).

- *Plant stability.* Check that the end point chosen for the accident sequence success represents a stable plant state.

2.5 Fault Trees

Objectives

The main objectives of the fault tree review are the following:

- To check whether the fault trees adequately represent the frontline systems as far as their failure modes are concerned. In particular, check the contributions from:
  - Hardware failures
  - Test and maintenance
  - Human errors
  - Support systems failures (in accordance with the method used in the event tree construction)
- To check whether the identified dependencies are correctly reflected in the fault trees.

The checklist items are cross-referenced with the applicable ASME standard (Ref. 4.7-1) index number(s).

Review Checklist

☐ ***Modeling assumptions.*** Check whether generic SPAR model fault tree assumptions are consistently used in the new or modified fault trees, as applicable.

Refer to the plant-specific SPAR model manual section, "Fault Tree Models," for fault tree modeling assumptions.

☐ ***System description***.

- o *Documentation.* Check for the use of appropriate plant information used in the construction or modification of the fault tree. (SY-A2)
- o *Walk downs/interviews.* Check whether system walk down and/or interviews with knowledgeable NRC staff or plant personnel were performed to confirm that the system analysis correctly reflects the as-built, as-operated plant. (SY-A4)

☐ ***System modeling.***

- *Modeling method.* Check how the system was modeled, e.g., detailed system model, single data value, supercomponent model. (SY-A7)

- *System boundaries.* Check the system boundary definition, including

  – Components within the boundary that are required for system operation.

  – Support systems interface required for actuation and operation of the system components.

  – Other components whose failures would degrade or fail the system. (SY-A6)

- Check whether the equipment and components whose failure would affect system operability (as identified in the system success criteria) was included in the fault tree model. This equipment includes both active components and passive components. (SY-A12)

- *Component boundaries.* Check that the component boundary definitions are consistent with the definitions used to collect the component failure data. (SY-A8)

- *Supercomponents.* Check for the use of supercomponent events. Check for irregularities in the event grouping of the supercomponent. (SY-A10)

  Examples include

  – Events with different recovery potential.
  – Events that are required by other systems (i.e., fault trees).
  – Events that have probabilities that are dependent on the scenario.

- *Multiple success criteria.* Check for the effect of variable or multiple success criteria of a system. (SY-A11)

  Examples of causes of variable system success criteria include

  – Different accident scenarios

- Dependence on other components
- Time dependence
- Sharing of a system between units when both units are challenged by the same initiating event

o *System isolation or trip signals.* Check for conditions that cause the system to isolate or trip, or conditions that once exceeded cause the system to fail. (SY-A17)

Example conditions that isolate or trip a system include:

- System-related parameters such as high temperature within the system.
- External parameters used to protect the system from other failures, e.g., high reactor pressure vessel water level isolation signal used to prevent water intrusion into the turbines of the reactor core isolation cooling (RCIC) and high-pressure core injection (HPCI) pumps in a boiling water reactor (BWR).
- Adverse environmental conditions.

o *Mission time.* Check for system conditions that cause a loss of desired system function for the required mission time, e.g., excessive heat loads, excessive electrical loads. (SY-A19)

o *System alignments.* Check for other conditions that prevent the system from meeting the desired system function, including the effects of both normal and alternate system alignments. (SY-A5)

o *System operation beyond rated or design capabilities.* Check for the credit of a system or component operability that is beyond rated or design capabilities.

Note: The ASME PRA standard does not credit such assumptions, unless justifications are provided. (SY-A20)

☐ ***Failure modes.***

o *Known failure modes.* Check that all known failure modes, especially common-cause failures, associated with the plant design have been considered during the fault tree development. (SY-A13)

- *Model construction*. Check that failure modes are properly positioned in the fault tree.

- *Beneficial failure modes.* Check for the inappropriate use of a failure mode that would be beneficial to system operation. Review the justification for the inclusion. (SY-A12)

- *Component testing.* Check that important components are periodically tested for the failure modes modeled in the fault tree. There may be some obscure failure modes that are missed during normal surveillance.

- *Operating experience.* Check that failure modes are consistent with available data—generic and plant-specific experience. (SY-A13)

- *NRC risk studies.* Check the fault tree for unique failure modes that were identified in the NRC system and component reliability studies. NRC risk studies can be viewed from the Reactor Operational Experience Results and Databases Web page (Ref. 4.2-1)

- *Exclusions.* Check for failure modes that were excluded from the fault tree based on screening criteria. Check the basis and evaluate the reasonableness of the removal. (SY-A14)

☐ ***Pre-initiator human events.*** (SY-A15)

- *Event inclusion.* Check the use of pre-initiator human events.

- *Data collection.* Check for "double counting" of failure events use in the calculations of the equipment failure probability and pre-initiator-human error probability.

- For example, if a pre-initiator human event is modeled separately in a system fault tree, then the related equipment failure probability should not include failure events from pre-initiator human actions in the failure estimation of the equipment.

☐ ***Post-initiator operator actions.***

- *Event inclusion.* Check the use of post-initiator human events. (SY-A16)

- *Manual actions.* Check that manual system or component actions are included either in the fault tree or event tree.

- *Procedures.* Check that an operating procedure requires the post-initiator action.

☐ ***Fail-to-restart.*** Check the use of a system restart model. For example, a system that is often restarted is RCIC. This system will trip off when high reactor water level is reached.

☐ ***Flow diversions.*** Fault trees typically model failure to provide flow from point A to point B, or flow diversion from A to B. Check whether both are present. This should include both liquid and gas flows and electric currents.

SPAR MODEL NOTE: Flow diversions are not normally modeled in SPAR models unless they involve failure of active components to transfer state, i.e., a normally open valve must close to prevent the diversion. Rupture or spurious transfer of a valve in a diversion path would not be modeled.

☐ ***Support system.***

- *System dependencies.* Check for dependencies between frontline safety systems and support systems. (SY-B5)
- *Support system dependencies.* Check for dependencies between support systems.
- *Fault tree construction.* Check that the support system was properly positioned in the frontline system fault tree.
- *Logic loops.* Check for undesirable logic loops in support system dependencies.
- *Mission times.* Check that the mission times for the frontline and support systems are compatible.
- *Inventories and resources.* Check the ability of the available inventories of air, power, and cooling to support the mission time of the system. (SY-B12)

☐ ***Environmental hazards.*** Check whether environmental hazards that may impact system operations are included in the system fault tree or event tree. The hazards can be caused by the initiator or during the accident progression. (SY-B8, SY-B15)

☐ ***Common-cause failure (CCF).***

- *CCF model.* Check how the CCF have been considered and modeled. (SY-B1)

- *Component groupings or CCCG.* Check the CCF grouping of components (i.e., common cause component group or CCCG) in the system based on the following similarities: (SY-B3)

  – Service conditions
  – Environment
  – Design or manufacturer
  – Maintenance

- *Fault tree construction.* Check that the CCF event was properly positioned in the fault tree.

- *CCF data collection.* Check that CCFs in the system model are consistent with the common cause model used for data analysis. (SY-B4)

- *Unique failure modes.* If a unique failure mode was modeled separately from the normal mode (e.g., fail-to-start, fail-to-run), then check how the CCF portion of the unique failure mode was modeled in the fault tree.

- *Exclusions.* If a component was excluded from the common cause component group, then check the basis and evaluate the reasonableness of the removal.

- *Inter-system CCFs.* Check whether inter-system CCFs are included in the model. Such CCFs are across systems performing the same function. (SY-B2)

SPAR NOTE: Inter-system CCFs are not typically included in SPAR models.

☐ ***Maintenance and test unavailability.***

- Check the modeling of out-of-service unavailability for components in the system. Unavailability can be due to testing or maintenance activities. (SY-A18)

- Check for screening of maintenance and test activities that could simultaneously have an impact on multiple trains of a redundant system or diverse systems. (HR-B1, HR-B2)

Note: The ASME PRA standard does not permit the screen of activities that could simultaneously have an impact on multiple trains of a redundant system or diverse systems.

☐ ***Recovery and repair.***

- o *System recovery.* If system recovery was not modeled in the event tree, then check whether system recovery was credited in the fault tree.

- o *Equipment repairs.* Check the use of hardware failure repair events. Check the basis of the repair events in the model, such as recovery analysis or review of operating experience data. (SY-A22)

- o See the checklist for non-recovery probability estimations.

☐ ***Logic gates.*** Check the "AND" and "OR" gate logic of the fault trees to ensure that the gates properly reflect the parallel/series arrangement of the components within the systems.

☐ ***Fault tree logic loops.*** Check how and where fault tree logic loops were cut to ensure that no important cut sets were omitted. Common loops include:

- o Diesel/service water/diesel
- o Diesel/room ventilation/diesel
- o Ac/dc/ac

☐ ***Shared components.***

- o *Inter-unit dependencies.* At sites where components and equipment are shared by more than one unit, check how inter-unit dependencies have been modeled in the fault trees.

- o *Inter-system dependencies.* Check how inter-system dependencies haven been modeled for shared components and equipment. (SY-A8, SY-B14)

☐ ***Basic event parameters.***

- o *Probability values.* Check that the probabilities of all basic events of the fault tree are given. (DA-A1)

- o *Undeveloped events.* Check for undeveloped basic events and the justification for not further developing the events.

- *Data entries.* Check that the basic event parameters (failure and uncertainty data) are not missing any data entries.

- *Calculation formulas.* Check that the basic event probability calculation is consistent with the identified failure mode.

- See the checklist for parameter estimations.

2.6 Parameter Estimations

Objective

The objective of this part of the review is to check the validity of point values and corresponding uncertainties for the parameters necessary for the quantification of accident sequences. These parameters include:

- Initiating event frequencies
- Component basic event probabilities

Case-by-case review of the basic event data would be time consuming and most likely yield limited results. This review checklist should be applied to the template data set each time a new SPAR model parameter file is released.

A case-by-case review should be performed for the following cases:

- Parameters that do not use template data
- Parameters for which the template data is not appropriate
- Modification of an existing parameter
- Creation of a new parameter specific for an analysis

The checklist items are cross-referenced with the applicable ASME standard (Ref. 4.7-1) index number(s).

Review Checklist

☐ ***Generic data collection.***

- *Data sources.* Check the source(s) of data used in the parameter estimation. (DA-A3)

- *Time period.* Check the time period of the data population for the following:

  – Consistency across parameters
  – Data exclusion
  – Very old operating experience

- *Other data.* Check for more complete sources of data in the desired population and during the desired time period.

- *Data exclusion.* Check the justification for the use or exclusion of historical data. (IE-C1)

- *Data exclusion.* If an event was appropriately excluded from the data pool, check that the associated demands, run time, reactor critical years were also excluded from the denominator of the estimate. If not, review the justification.

- *Component groupings.* Check the component grouping of the data according to component type (e.g., motor-operated pump, air-operated valve) and according to the detailed characteristics of their usage.

Component characteristics include:

  – Design/size

  – System characteristics. Examples include: mission type (e.g., standby, operating), service condition (e.g., clean vs. untreated water, air), maintenance practices, frequency of demands

  – Environmental conditions

  – Other appropriate characteristics

  Note: The ASME PRA standard does not permit the inclusion of outliers in the definition of a component group (e.g., grouping valves that are never tested and unlikely to be operated with those that are tested or otherwise manipulated frequently). (DA-B1, DA-B2)

- o *Outdated data.* Check for modifications to plant design or operating practice that led to a condition where past data are no longer representative of current performance. (DA-D7)

- o *Data classifications.* If possible review a sample of the Licensee Event Reports (LERs) or other information from which failure probabilities were derived to ensure that the failure events were properly classified, in accordance with the parameter definition.

- o Note: This check is important for rare or infrequent events.

- o *EPIX data.* If data from the Equipment Performance and Information Exchange (EPIX) database was used, check for data inconsistency between plants.

☐ ***Plant-specific data collection.***

- o Check whether a plant-specific database was used. Review a sample of the records for adequate classification, in accordance with the parameter definition.

- o If plant-specific estimates were used, then check (to the extent possible) the basis for using industry-average estimates in the model, as applicable.

- o If EPIX data was used in the parameter estimation, then check for data inconsistency between the plant-specific data and the industry-average data (e.g., the plant has fewer events and demands than most plants).

- o If plant-specific data was used to update an industry-average parameter estimate, then check that the data conforms to the parameter definition.

- o If the SPAR model was modified to analyze the operational event, check that the parameter estimation conforms to the SPAR model success criteria, description, and philosophy.

☐ ***Multiple databases.*** If more than one database was used, check for any apparent bias in their use. For example, check for plant-specific parameter values that are lower than the corresponding generic values.

☐ ***Infrequent or rare events.***

- For cases where neither plant-specific data nor generic parameter estimates are available, check the use of data or parameter estimates from similar components or the use of expert judgment.

- Check that the data used to estimate probabilities or frequencies for rare events are applicable to the SPAR model definitions and assumptions.

☐ ***Statistical methods.***

The following reviews of statistical methods should be performed by a knowledgeable statistician.

- *Data reduction.* Check the statistical techniques used for data reduction, e.g., time trend analysis. (IE-C5)

- *Probability model.* Check the probability model used for each basic event. (DA-A2)

- *Prior distribution.* If a Bayesian approach was followed, check the reasonableness of the prior distribution. (DA-D1)

- *Mean and uncertainty.* Check that the parameter estimate includes a mean value and an uncertainty interval.

- *Bayesian approach.* If a Bayesian approach was used to derive a distribution and mean value of a parameter, then check the following to ensure that the updating is accomplished correctly and that the generic parameter estimates are consistent with the plant-specific application (DA-D6):

  – Check that the Bayesian updating does not produce a posterior distribution with a single bin histogram.

  – Check the cause of any unusual posterior distribution shapes.

  – Check inconsistencies between the prior distribution and the plant-specific evidence to confirm that they are appropriate.

  - Check that the Bayesian updating algorithm provides valid results over the range of values being considered.

  - Check the reasonableness of the posterior distribution mean value.

- *Varying statistical approaches.* Check whether the statistical approach used in the parameter estimation was the same for other parameters. If not, then review the justification for any differences.

- *Time periods.* If the time periods in the data vary among similar parameters, then check the statistical method used to justify a shorter or longer time period where applicable.

- Deviations. Check for deviations from data collection and statistical methods normally used for estimating SPAR model parameters. Check whether such deviations have been reviewed by knowledgeable statisticians and data collectors.

☐ ***Calculation formulas.***

- *Proper formulas.* Check that the basic event probability calculation is consistent with the identified failure mode.

- *Formula input(s).* Check that the numerical values of the formula input(s) are consistent with the formula type.

- *Mission times.* Check that the parameter mission time (as applicable) is consistent with other components in the fault tree and in the fault trees in the sequence.

☐ ***Template events.*** Check that modifications to template events do not adversely impact the wrong basic events.

Template events are basic events that most often represent a particular failure mode for a particular component type (i.e., check valve fails to open, motor operated valve fails to close, etc.). A modification of a template event will affect several basic events.

☐ ***Compound events.*** Check that modifications to a basic event do not adversely impact a compound event.

Compound events can be viewed as supercomponent basic events which combine other basic events according to some rule or equation to obtain a failure probability. The

compound event feature is used primarily to minimize the number of basic events in the cut sets, while also allowing automated uncertainty analysis.

A common problem with compound events is setting an independent event in a common cause component group to a probability different from that of the other members of the group. Unless the value is 1.0 or "TRUE", both of which have special meanings in the SAPHIRE code, the common cause failure calculation is not defined and will result in the related common cause event being set to 1.0. This will change in SAPHIRE Version 8, but is still true for all SAPHIRE Version 7 models.

☐ ***Initiating event frequencies.***

- *Initiator groupings.* Check the grouping of initiators in a parameter estimate. For example, combining the contribution of all small LOCA initiators into one parameter, e.g., pipe breaks, stuck open relief valves. (IE-B3)

- *Recovery.* Check whether the initiating event frequency includes recovery and whether this approach matches the event tree definition. (IE-C1)

- *Initiator exclusions.* Check whether the initiating event has been screened out in the SPAR model, but may be important in the analysis of the operational event. (IE-A6, IE-C1)

- *Plant specific vs. industry average.* If an industry average frequency was used, then check for a plant-specific initiator occurrence rate that is higher than the industry average.

- *Data exclusions.* Check the justification of excluded data that is not considered to be either recent or applicable, e.g., provide evidence via design or operational change that the data are no longer applicable. (IE-C1)

- *Multi-unit site initiators.* Check for multi-unit site initiators, such as dual unit LOOP events or total loss of service water that may impact the model at multi-unit sites with shared systems. (IE-A10)

☐ ***Initiating event fault tree model.***

- *System analysis.* When the fault-tree approach was used to quantify an initiating event frequency, check the system analysis used to develop the fault tree. (IE-C6)

- *Quantification.* Check that the fault tree quantification method produces a failure frequency rather than a top event probability. (IE-C7)

- *Component unavailabilities.* Check within the initiating event fault tree model that all relevant combinations of events involving the annual frequency of one component failure combined with the unavailability (or failure during the repair time of the first component) of other components. (IE-C8)

- *Recovery actions.* Check that plant-specific information was used in the assessment and quantification of recovery actions where available. (IE-C9)

- *Reasonableness checks.* Check the results of the initiating event analysis with generic data sources to provide a reasonableness check of the results. For example, an operational event observed in the operating experience data should be considered in the fault tree model. (IE-C10)

☐ ***Unavailability estimates.***

- *Plant status.* Check that the unavailability estimates reflect the equipment outage time during the desired plant status (e.g., at power, cold shutdown, refueling). (DA-C12)

- *Multi-unit sites.* Special attention should be paid to the case of a multi-unit site with shared systems, when the Technical Specifications (TS) requirements can be different depending on the status of both plants. Check the treatment of the allocation of outage data among basic events to take this mode dependence into account. (DA-C12)

- *Operating experience.* Check for coincident outage times for redundant equipment (both intra- and inter-system) based on actual plant experience. (DA-C13)

☐ ***CCF probabilities.***

- *CCF method.* Check that the CCF method used to estimate the CCF parameter is consistent with the method used in SPAR models. If an alternative method is used, then check the justification (i.e., evidence of peer review or verification of the method that demonstrates its acceptability). (DA-D5)

- *CCF database.* Check that both the CCF events and the independent failure events in the data base used to generate the CCF parameters are consistent with the plant design and operational characteristics, as well as available plant experience. (DA-D6)

- o *Data exclusions.* Check that the records excluded or screened from the data pool used to generate the CCF parameters are appropriately justified. (DA-D6a)

- o *SAPHIRE calculations.* Check that the CCF probability was properly calculated in SAPHIRE given the following:

  - – Observed failure (e.g., fail-to-start, fail-to-run)
  - – Observed unavailability (i.e., component in test or maintenance).

☐ ***Standby components.*** Check for fault exposure times (standby components).

☐ ***Results.***

- o *Unit of measure*. Check the unit of measure (e.g., per reactor critical year, failure per hour)

- o *Rounding.* Check rounding that reflects the precision of the results.

☐ ***Differences with the plant PRA.*** Review any noted differences with parameter values between the plant PRA and SPAR model. Check for adequate justifications.

2.7 Non-Recovery Probability Estimation Checklist

Objective

The objective of this part of the review is to check the modeling of system recovery.

The checklist items are cross-referenced with the applicable ASME standard (Ref. 4.7-1) index number(s).

Review Checklist

☐ ***Recovery models.***

- o Check that the system recovery model used to estimate the non-recovery probability is consistent with the application.

- Check that the data used in the system recovery model is consistent with the application (e.g., LOOP, EDG).

☐ ***HRA method.*** Check the human reliability analysis method used to estimate the non-recovery probability is consistent with the application.

☐ ***Conditional non-recovery probabilities.*** Check whether conditional non-recovery probabilities are properly modeled in a sequence.

☐ ***Non-recovery probability < failure probability?*** If recovery is included in the system fault tree, check whether too much credit for recovery has been given in regard to the sequences in which the system must operate.

☐ ***Basic events***. Check that non-recovery basic events included in the fault trees that appear in the cut sets have appropriate assigned probabilities, considering the cut set structure.

2.8 Know Where the Basic Event or Fault Tree Is Used in the SPAR Model

Objective

The objective of this part of the review is to ensure that changes to a basic event or fault tree do not adversely impact other parts of the SPAR model.

Review Checklist

☐ Check that a proposed change in a basic event parameter (e.g., failure probability, mission time, calculation type, and process flag) does not adversely impact the use of the same basic event used elsewhere in the SPAR model. The change may not be appropriate in all sequences.

For example, a degraded component may not have enough capacity for one sequence (thus the reason for setting the basic event to TRUE), but may have enough capacity for success in another event tree sequence.

☐ Examples where changes to a basic event parameter can effect multiple parts of the model include:

- Basic event used in multiple fault trees.
- Basic event used as an input to a compound event.
- Template event shared by basic events of a component group.

- o Basic event used in recovery rules.

☐ Check that a change in a fault tree (e.g., modification, addition, deletion, replacement) does not adversely impact another sequence in the SPAR model.

- o Examples where changes to a fault tree can effect multiple parts of the model include:

- o Same fault tree may be used in different event trees.

- o Variations of a system fault tree may be used in recovery rules applied to the same event tree sequence (e.g., different success criteria).

☐ To view where the basic event is used, in SAPHIRE Version 7:

- o Select *Modify.*

- o Select *Basic Event.* (Note: Any basic event in the fault tree including the top event is provided in the list.)

- o Select the basic event name from the *Edit Events* window.

- o Select *Cross Reference.*

2.9 Model Solution Review

Objective

The objectives of this part of the review are the following:

- To review inputs and modifications to the SPAR model.
- To review model solution (quantification) results.

The checklist items are cross-referenced with the applicable ASME standard (Ref. 4.7-1) index number(s).

Review Checklist

☐ ***Model modification documentation.*** Check that the documentation of model modifications matches the revised baseline SPAR model. Review the modifications of the following:

- o Success criteria
- o Event trees
- o Event tree linking rule
- o Event tree process flag
- o Fault trees
- o Recovery rules
- o Basic events
- o Parameter values

☐ ***Truncation input.*** Check the truncation probability used in the model solution is sufficient for the application.

☐ ***Analysis inputs.***

- o *Parameter values.* Check for the proper use of parameter value representing a failure or unavailable basic event (e.g., “TRUE” vs. 1.0).

- o *Know where the modified basic event is used.* Check that changes in a basic event input parameter does not adversely impact the use of the same basic event elsewhere in the SPAR model. Examples where changes to a parameter can effect multiple parts of the model include:

  - – Basic event used in different fault trees.
  - – Basic event used in a compound event.
  - – Template event shared by basic events of a component group.
  - – Basic event used in recovery rules.

☐ ***Condition exposure time input.*** Check the exposure time of the failed or degraded SSC condition.

☐ ***Cut set reviews.***

- o Compare the revised model sequence cut sets with those from the original SPAR model to confirm model revisions.

- o Check that the results are consistent with the failures, unavailabilities and off-normal conditions that were observed in the operational event.

- o Check that the probabilities for sequences adversely impacted by the condition or event is higher in probability than in the base case model.

- o Check that no sequences that were conservatively or simplistically developed in the original SPAR model exist among the dominant sequences.

- o Check that no basic events impacted by a component failure appear in an unmodified form unless this is appropriate for the event.

- o Check that a basic event used to model a component failure is not included in a recovery rule. Setting a basic event used in a recovery rule to "TRUE" will cause the event to be unavailable to the recovery rule processor. The results will be unpredictable and could involve failure to apply a valid recovery, failure to eliminate a TS disallowed condition, failure to apply a human error dependency, etc.

- o Check that components supported by another failed component or train (e.g., a pump supported by an observed failed cooling water train) have been removed from the dominant cut sets.

- o Check that basic events expected to be contributors to dominant cut sets is included in those cut sets.

- o Check that basic events added or increased in probability to reflect the condition or event (e.g., the CCF probability associated with a failed component) are appropriately reflected in the dominant cut sets.

- o Check for multiple recovery events in a cut set.

- o Check for mutually exclusive basic event combinations that may appear due to simplified model logic.

Note: Use caution when deleting multiple train test and maintenance (T/M) combinations; such combinations have occasionally been observed in the operating experience data.

☐ ***Importance measures review.*** Using the risk achievement and risk reduction importance measures associated with the conditional cut sets, check that:

- o Basic events expected to be important based on the failures and off-normal conditions observed during the condition or event are, in fact, important.

- o Probabilities of important basic events are reasonable and justifiable.

☐ ***Model uncertainties.*** Check that risk important uncertainties in the SPAR model assumptions and technical issues have been addressed in the model or documentation.

☐ ***Reasonableness reviews***. Do the initial results appear to be appropriate based on the analyst's understanding of plant operation and risk-important features?

SPAR Model Reviews: Key Assumptions and Technical Issues	Section 3 Rev. 2

3.0 Key Assumptions and Technical Issues

3.1 General Notes

☐ Generic and plant-specific SPAR model assumptions are documented in the plant SPAR model manual.

☐ The risk importance ranking of known model assumptions depends on the operational event and sequences of interest. Only some baseline differences between the SPAR and plant PRA models may be important in a particular analysis of an operational event.

3.2 Frequencies and Probabilities

☐ ***Generic parameter estimates*** (failure probabilities and initiating event frequencies) based on generic industry average data from NUREG/CR-6928.

☐ ***Common-cause failure*** not modeled across systems.

☐ ***Emergency diesel generators*** typically modeled with a 24-hour mission time.

☐ ***Failure to run parameters*** occurs at time zero.

Convolution has been applied to all models for the EDG. TDP have not been done but will be considered on a case by case basis.

☐ ***Large and medium LOCA*** frequencies based on NUREG/CR-5750 (to be updated with pending final NUREG-1829).

(Technical issue pending resolution)

☐ ***Support system*** initiating event frequencies (i.e., service water, component cooling water, instrument air, electrical bus) based on point estimates.[1]

(Technical issue pending resolution)

3.3 Failure Data Assumptions

☐ **The official version** of the SPAR model includes industry-average performance data (for basic events and initiating events) developed recently. These data reflect industry-average performance centered about the year 2000. Updated failure data values have been incorporated into all SPAR models. Data will continue to be updated on a periodic basis.

☐ **Generic parameter estimates** (failure probabilities and initiating event frequencies) based on generic industry average data from NUREG/CR-6928.

☐ **Failure to run parameters** occur at time zero. Convolving the failure distributions of time based failures during LOOP/SBO events eliminates the simplifying assumption that all failures to run/operate happen at time = 0. A methodology and related data values (template events) have been developed. This information will not be applied until after the detailed PRA cut set level reviews are completed. At that time this information/modification will be added to all models at once. (Convolution of failure to run will be applied to EDGs).

☐ **Updated Alpha Factor data** have been incorporated into all SPAR models. Data will continue to be updated on a periodic basis.

☐ **Relief valve (SRV, PORV, ADS)** challenge and failure rates are not plant or initiator specific.

☐ **Large and medium LOCA frequencies** are based on NUREG/CR-5750 (to be updated with pending final NUREG-1829).

☐ **Support system initiating event frequencies** (i.e., service water, component cooling water, instrument air, electrical bus) are based on point estimates (Point estimates underestimates event importances. Use of fault trees that accounts for specific system configurations is being implemented.)

1. Point estimates underestimates event importance. Use of fault trees that accounts for specific system configurations is under investigation.

3.4 System Modeling

☐ ***Instrumentation and control*** not explicitly modeled (implicit in data).

☐ ***Service water*** environmental issues (water quality) not modeled.

☐ ***One SPAR model*** for some multi-unit sites.

☐ ***Electrical power distribution systems*** may have limited modeling details.

☐ ***Alternate/backup electrical power sources*** may be modeled with preferential alignments.[2]

☐ ***Balance-of-plant systems*** and associated support systems may have limited modeling details.

(Technical issue pending resolution)

☐ ***Containment sump*** (PWR) and ***suppression pool strainer*** (BWR) plugging probabilities based on generic values (GSI 191 issue).

(Technical issue pending resolution)

☐ ***Station blackout*** sequence timing to core uncovery for various scenarios based on existing generic thermal hydraulic analysis.[3]

(Technical issue pending resolution)

☐ **Only failure of major components** (pumps, valves, heat exchangers, etc.) identified in the system P&IDs will be considered. Also, only hardware, human error, and common mode failures will be considered. Spurious actuation or trip events are not modeled. This includes the spurious opening or closing of boundary valves and full-flow test line isolation valves during the course of the system demand. Failure of the automatic actuation circuitry is modeled as a single basic event, if deemed necessary. Service water environmental issues

2. Plants with extremely large logic for multiple cross-tie capabilities and/or sources may be modeled with the most common combinations.

3. Thermal-hydraulic analyses include NUREG/CR-4471, NUREG/CR-2182, NUREG/CR-5565, NUREG-1032.

(water quality) not modeled. Shared plant models exist for some SPAR models at multi-unit sites. Electrical power distribution systems may have limited modeling details.

☐ Alternate/backup electrical power sources may be modeled with preferential alignments. Plants with extremely large logic for multiple cross-tie capabilities and/or sources may be modeled with the most common combinations.

☐ **SAPHIRE project recovery rules** remove combinations of test and maintenance events that are disallowed by the plant Technical Specifications. The cut sets that must be removed are identified in the output of the ME-TECHSPEC fault tree.

3.5 Generic BWR System Modeling Assumptions

Generic modeling assumptions for BWR SPAR models are summarized below. The fault tree assumptions may not apply to all models.

☐ **Condensate system.** Feedwater pump flow paths will be lost. The operators will open the feedwater pump bypass line for condensate injection. This is a pessimistic assumption resulting from uncertainty over how much flow could be obtained through possibly failed reactor feedwater pumps.

☐ **Control rod drive system.** Valves and piping down-stream of the cooling water and charging headers are not included in the model. There is sufficient redundancy to neglect the additional components.

☐ **High-pressure coolant injection (HPCI).** The model assumes that HPCI is initially aligned to take suction from the condensate storage tank. The model assumes that realignment of suction to the suppression pool will eventually be required. The HPCI fault tree model is based on the RES HPCI system reliability study.[4] The system boundaries include the turbine and turbine control valves, coolant piping and valves, instrumentation and control, circuit breakers at the motor control centers, the dedicated dc power system that supplies HPCI system power, heating, ventilating and air conditioning systems and room cooling associated with HPCI.

☐ **High-pressure core spray (HPCS).** The model assumes that HPCS is initially aligned to take suction from the condensate storage tank. The model assumes that realignment of suction to the suppression pool will eventually be required.

4. U.S. Nuclear Regulatory Commission,, “High-Pressure Safety Injection System Reliability, 1987-1997 (DRAFT),” INEEL/EXT-99-00373, NUREG/CR-XXXX (DRAFT), July 1999.

- **Reactor core isolation cooling injection (RCIC).** The RCIC fault tree model is based on the RES RCIC system reliability study. The system boundaries include the turbine and turbine control valves, coolant piping and valves, instrumentation and control, circuit breakers at the motor control centers, the dedicated dc power system that supplies RCIC system power, heating, ventilating and air conditioning systems and room cooling associated with RCIC.

- **Reactor shutdown.** Success requires insertion of the minimum number of control rods.

3.6 Generic PWR System Modeling Assumptions

Generic modeling assumptions for PWR SPAR models are summarized below. The fault trees assumptions may not apply to all models.

- **Component cooling/service water.** Automatic actuation system dependencies and make-up water to the component cooling tank are not included in the model.

- **AC and DC buses.** Testing/maintenance unavailabilities, post-accident human errors and manually-aligned cross-connects are generally not included in the model.

- **Main feedwater (MFW).** For the SPAR model, it will be assumed that the MFW system will isolate given an SI signal and an operator action will be modeled to re-align the flow to the steam generators. For general transients, MFW assumptions are:

  The MFW system is normally operating.

  For most Westinghouse plant designs, after the reactor trips, the MFW will isolate on a low T_{ave}. The dominant factor in the system operability can be modeled by an operator action to restore the MFW flow to the steam generators. Therefore, MFW and condensate system hardware failures are not explicitly modeled.

  For other plant designs, given a reactor trip, the MFW system will ramp back and continue to provide flow to the steam generators unless the transient is a loss of MFW.

  MFW and condensate system hardware failures are not (typically explicitly modeled, but are rolled up into a single event representing the likelihood of the transient being a loss of MFW. However, as part of the detailed PRA cut set level review, the level of detail of the BOP systems is being expanded to include basic support systems and key equipment.

- **MFW assumptions during an ATWS are:**

  The MFW system is normally operating.

  The MFW will not receive any isolation signal given the reactor failed to trip and continue to provide flow to the steam generators.

  The system failure probability is based solely upon the transient being a loss of MFW and no operator recovery is available due to the timing of events. However, as part of the detailed

PRA cut set level review, the level of detail of the BOP systems is being expanded to include basic support systems and key equipment.

☐ **MFW assumptions during non-transients** [e.g., Small loss-of-coolant accident (LOCA), steam generator tube rupture (SGTR)] are:

The MFW system is normally operating.

Upon a safety injection signal, the MFW system will isolate.

The dominant factor in the system operability can be modeled by an operator action to restore the MFW flow to the steam generators. Therefore, MFW and condensate system hardware failures are not explicitly modeled. However, as part of the detailed PRA cut set level review, the level of detail of the BOP systems is being expanded to include basic support systems and key equipment.

☐ **Feed and bleed.** All SPAR models currently require two PORVs to open for successful bleed and feed. This criterion may be reduced on a plant specific basis if sufficient justification (i.e., detailed plant specific thermal hydraulic calculations) is made available by the licensee and/or confirmed by RES thermal-hydraulic analyses.[5] Detailed plant/class specific analyses are being considered.

☐ **Reactor trip.** This fault tree represents failure of the reactor protection system to scram the reactor when required. Operator action to manually scram the reactor is modeled. The operator action includes failure to manually scram the reactor for those failures for which manual action can affect scram (i.e., electrical failures). Reactor Trip System failures are dominated by trip breakers and control rod drives.

3.7 Recovery Modeling

☐ ***Support system*** initiators (e.g., loss of service water, loss of electrical bus) may have limited recovery modeling.

☐ ***Turbine-driven pump*** operations not credited without dc power (manual control typically not credited).

☐ ***System hardware*** may have limited modeling of recovery and repair actions.

5. U.S. Nuclear Regulatory Commission,, “Confirmatory Thermal-Hydraulic Analysis to Support Specific Success Criteria in the Standardized Plant Analysis Risk Models – Surry and Peach Bottom,” NUREG/CR-XXXX (DRAFT), August 2010.

☐ ***Station blackout*** sequences credit no recovery of ac electrical power after battery depletion.[6]

(Technical issue pending resolution)

☐ ***Charging and safety injection pumps*** may have limited modeling of alternate component cooling to preclude reactor coolant pump seal failure.

(Technical issue pending resolution)

3.8 Human Error Modeling

☐ ***Errors of commission*** are typically not modeled.

☐ ***Diagnosis*** success implied for all sequences (with the exception of steam generator tube rupture sequences).

☐ ***Pre-accident human errors*** not explicitly modeled (implicit in data).

SPAR NOTE: some SPAR models still contain many XHE-XR events. These fail-to-restore events might be considered a valid part of the fail-to-start data for a given component. Pre-accident failures to restore systems following test or maintenance (T/M) are quantified using generic ASEP data, data from NUREG-1150, and engineering judgment.

☐ ***Human error probabilities*** estimated using the SPAR-H human reliability analysis method.

(Technical issue pending resolution)

---

6. Issues for considerations include:

- Diesel-driven injection sources
- Availability and quality of procedural guidance
- Training
- Capacity of water sources for continued injection
- Room heatup and other environmental concerns
- Duration of emergency lighting
- Switchyard battery life and recharge capability

- **Post-Accident Failures to Align Systems and Control /Operate Systems.** This post-accident failures model includes operator actions to manually align systems and to control or operate systems. Human error probabilities (HEPs) for these types of actions have generally been calculated using the SPAR-H human error worksheets.

- **Human error dependency modeling.** In the SPAR models, the operator error events are first evaluated without considering dependence then, after solution of the core damage equations, event substitutions are used to account for dependency between events in a given cut set.

- **Recovery of System Hardware Failures.** Nominal recovery credited in SPAR models. This assumption is similar to most full scope PRAs and IPEs in that nominal recovery of hardware failures is not generally credited. There are some exceptions as discussed below.

- **The loss of offsite power** (LOOP) and station blackout (SBO) models consider recovery of AC power in detail.

- **Recovery dependency modeling.** Dependency among these hardware recovery events was taken into account. It was assumed that the recovery events were completely dependent upon one another and only one hardware recovery could be performed per cut set. Therefore, multiple hardware recovery events from the same system were pruned down to contain only one per cut set.

3.9 Standard Human Actions in SPAR

- The following are the Standard BWR events and descriptions used with SPAR-H.

ADS-XHE-XM-MDEPR Operator fails to depressurize the Reactor

This human failure event starts from full power operation. Diagnosis of the need for the operator to depressurize the reactor is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action, the stress level and the complexity are nominal. The experience/training is high due to the assumption that the training and experience happens often. The procedures, the ergonomics/Human Machine Interface (HMI), fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

CDS-XHE-XO-ERROR Operator fails to start/control Condensate Injection

This human failure event starts from full power operation. Diagnosis of the need for control of condensate injection is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

CVS-XHE-XM-VENT Operator fails to vent Containment

This human failure event starts from full power operation. Diagnosis of the need for the operator to vent containment is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

HCI-XHE-XO-ERROR Operator fails to start/control High Pressure Coolant Injection (HPCI) Injection

This human failure event starts from full power operation. Diagnosis of the need for the operator to start/control HPCI injection is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

ISL-XHE-XD-DIAG Operator fails to diagnose Interfacing System Loss of Coolant Accident (ISLOCA)

This human failure event starts from full power operation. This event is for diagnosis only and the diagnosis can be difficult and involve numerous operators and support personnel. The time available for the action is nominal. The stress level is high because of the effort needed to determine that it is an interfacing LOCA. The complexity is moderately complex due to the coordination of the personnel involved in the diagnosis. The experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are nominal. Dependency is not modeled for this action.

ISL-XHE-XE-REC Operator fails to recover (isolate) Interfacing System Loss of Coolant Accident (ISLOCA) rupture

Diagnosis is not modeled because it was modeled separately in the ISL-XHE-XD-DIAG even but the action is modeled. The time available for the action is nominal. The stress level is high because of the effort needed to determine where the interfacing LOCA is occurring. The complexity is moderately complex due to the coordination of the effort to find the leak. The experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are nominal. Dependency is not modeled for this action.

MFW-XHE-XO-ERROR Operator fails to start/control Feedwater Injection

This human failure event starts from full power operation. Diagnosis of the need for the operator to start/control feedwater injection is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

OPR-XHE-XM-ADSINHIB Operator fails to inhibit ADS

This human failure event starts from full power operation. Diagnosis of the need for the operator to inhibit ADS is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

OPR-XHE-CTRL-TAF Operator fails to control level to Top of Active Fuel (TAF)

This human failure event starts from full power operation. Diagnosis of the need for the operator to control level to TAF is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action is nominal. The stress level is high due to controlling shrink and swell through indicators. The complexity is moderately complex. The experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

OPR-XHE-NOOVRFIL Operator fails to control Reactor Pressure Vessel (RPV) level

This human failure event starts from full power operation. Diagnosis of the need for the operator to not overfill the RPV is not

	modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.
PCS-XHE-XE-L1BYP	Operator fails to bypass Main Steam Isolation Valve (MSIV) level 1 trip This human failure event starts from full power operation. Diagnosis of the need for the operator to bypass the MSIV level 1 trip is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.
RCI-XHE-XO-ERROR	Operator fails to start/control Reactor Core Isolation Cooling (RCIC) Injection This human failure event starts from full power operation. Diagnosis of the need for the operator to start/control RCIC injection is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.
RHR-XHE-XM-ERROR	Operator fails to start/control RHR This human failure event starts from full power operation. Diagnosis of the need for the operator to start/control RHR is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action, stress level, and complexity are nominal. The experience/training is high due to the assumption that the training and experience happens often. The procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.
SDC-XHE-XM-ERROR	Operator fails to align Shutdown Cooling This human failure event starts from full power operation. Diagnosis of the need for the operator to align Shutdown cooling is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity is

moderately complex due to the alignment of Shutdown Cooling that must be done. The experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are nominal. Dependency is not modeled for this action.

SLC-XHE-XM-ERROR Operator fails to start/control Standby Liquid Control (SLC)

This human failure event starts from full power operation. Diagnosis of the need for the operator to start/control SLC is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action is nominal. The stress for this action is high because of the system being used during performance of this evolution. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

☐ The following are the Standard PWR events and descriptions used with SPAR-H.

AFW-XHE-XM-SGDEP Operator fails to depressurize SGs to atmospheric pressure

This human failure event starts from full power operation. Diagnosis of the need for depressurization is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action and the stress level are nominal. The complexity, the experience/training, the procedures, the ergonomics/Human Machine Interface (HMI), fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

CDS-XHE-XO-ERROR Operator fails to start/control Condensate Injection

This human failure event starts from full power operation. Diagnosis of the need for control of condensate injection is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

CVC-XHE-XM-BOR Operator fails to initiate Emergency Boration

This human failure event starts from full power operation. Diagnosis of the need for emergency boration is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available is just enough time because the assumption is that there is just enough time to perform function. The stress levels are high because the

assumption that having just enough time induces high stress for performance of this evolution. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

DHR-XHE-XM-ERROR Operator fails to initiate Decay Heat Removal/Shutdown Cooling (DHR/SDC) cooling mode

This human failure event starts from full power operation. Diagnosis of the need for initiating decay heat removal/shutdown cooling is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available is just enough time because the assumption is that there is just enough time to perform function. The stress levels are high because the assumption that having just enough time induces high stress for performance of this evolution. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

HPI-XHE-XM-FB Operator fails to initiate Feed and Bleed cooling

This human failure event starts from full power operation. Diagnosis of the need for initiating feed and bleed cooling is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available is just enough time because the assumption is that there is just enough time to perform function. The stress levels are high because the assumption that having just enough time induces high stress for performance of this evolution. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

HPI-XHE-XM-RWSTR Operator fails to refill the Refueling Water Storage Tank (RWST)

This human failure event starts from full power operation. Diagnosis of the need for operator needing to fill the RWST is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action and the stress level are nominal. The complexity, the experience/training, the procedures, the ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

HPI-XHE-XM-THRTL Operator fails to control/terminate Safety Injection flow

This human failure event starts from full power operation. Diagnosis of the need for operator needing control/terminate

Safety Injection flow is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action and the stress level are nominal. The complexity, the experience/training, the procedures, the ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

HPR-XHE-XM-RECIRC Operator fails to start High Pressure Recirculation

This human failure event starts from full power operation. Diagnosis of the need for operator to start high pressure recirculation is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action and the stress level are nominal. The complexity, the experience/training, the procedures, the ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

ISL-XHE-XD-DIAG Operator fails to diagnose Interfacing Systems Loss of Coolant Accident (ISLOCA)

This human failure event starts from full power operation. This event is for diagnosis only and the diagnosis can be difficult and involve numerous operators and support personnel. The time available for the action is nominal. The stress level is high because of the effort needed to determine that it is an interfacing LOCA. The complexity is moderately complex due to the coordination of the personnel involved in the diagnosis. The experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are nominal. Dependency is not modeled for this action.

ISL-XHE-XE-REC Operator fails to recover (isolate) ISLOCA rupture

Diagnosis is not modeled because it was modeled separately in the ISL-XHE-XD-DIAG even but the action is modeled. The time available for the action is nominal. The stress level is high because of the effort needed to determine where the interfacing LOCA is occurring. The complexity is moderately complex due to the coordination of the effort to find the leak. The experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are nominal. Dependency is not modeled for this action.

LPR-XHE-XM-RECIRC Operator fails to initiate Low Pressure Recirculation

This human failure event starts from full power operation. Diagnosis of the need for operator to start low pressure recirculation is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The

time available for the action and the stress level are nominal. The complexity, the experience/training, the procedures, the ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

MFW-XHE-XO-ERROR Operator fails to start/control Feedwater Injection

This human failure event starts from full power operation. Diagnosis of the need for starting/controlling feedwater injection is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for this action and stress levels are nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

MSS-XHE-XM-BLK Operator fails to close Automatic Depressurization Valve (ADV) block valve

This human failure event starts from full power operation. Diagnosis of the need for closing the ADV block valve is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available is just enough time because the assumption is that there is just enough time to perform function. The stress level is nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

MSS-XHE-XM-ERROR Operator fails to isolate faulted Steam Generator

This human failure event starts from full power operation. Diagnosis of the need for isolating faulted steam generator is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available is just enough time because the assumption is that there is just enough time to perform function. The stress level is nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

OPR-XHE-XM-RSSDEP Operator fails to cooldown Reactor Coolant System (RCS) to 1720 psi in 2 hours

This human failure event starts from full power operation. Diagnosis of the need for operator to cooldown the RCS to where the pressure is 1720 psi in two hours is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action and the stress level are nominal. The complexity, the experience/training,

the procedures, the ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

PCS-XHE-XM-CDOWN Operator fails to initiate Cooldown

This human failure event starts from full power operation. Diagnosis of the need for operator to initiate cooldown of the primary coolant system is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action and the stress level are nominal. The complexity, the experience/training, the procedures, the ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

PPR-XHE-XM-BLK Operator fails to close Pressurizer block valve

This human failure event starts from full power operation. Diagnosis of the need for the operator to close the pressurizer block valve is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action and the stress level are nominal. The complexity, the experience/training, the procedures, the ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

RCS-XHE-RECOVER Operator fails to depressurize RCS below SG Safety Relief Valve (SRV) given ADV or SRV opened

This human failure event starts from full power operation. Diagnosis of the need for the operator to depressurize the RCS below the SG SRV pressure given an ADV or SRV opened is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available is just enough time because the assumption is that there is just enough time to perform function. The stress level is nominal. The complexity, experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

RCS-XHE-XA-TRIP Operator fails to trip Reactor Coolant Pump (RCP) after loss of cooling

This human failure event starts from full power operation. Diagnosis of the need for the operator to trip the RCP after loss of cooling is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available is just enough time because the assumption is that there is just enough time to perform function. The stress level is nominal. The complexity is moderately complex because tripping

the RCP is the last thing an operator wants to do. The experience/training, procedures, ergonomics/HMI, fitness for duty, and work processes are nominal. Dependency is not modeled for this action.

RCS-XHE-XE-SGTR Operator fails to diagnose Steam Generator Tube Rupture (SGTR) and start procedures

This human failure event starts from full power operation. This event is for diagnosis and starting procedures only and the diagnosis can be difficult and involve numerous personnel. The time available for the action is nominal. The stress level is high because of the effort needed to determine which SG has a tube rupture. The complexity is moderately complex due to the coordination of the personnel involved in the diagnosis. The experience/training is high because this procedure is practiced on the simulator. The procedures are symptom oriented in order to have a better chance at diagnosis. The ergonomics/HMI and fitness for duty are nominal. The work processes are good. Dependency is not modeled for this action.

RHR-XHE-XM-ERROR Operator fails to initiate Residual Heat Removal (RHR) system

This human failure event starts from full power operation. Diagnosis of the need for the operator to initiate the RHR system is not modeled since the actions are proceduralized and the need for action is obvious but the action is modeled. The time available for the action and the stress level are nominal. The complexity, the experience/training, the procedures, the ergonomics/HMI, fitness for duty, and work processes are also nominal. Dependency is not modeled for this action.

SDC-XHE-XM-ERROR Operator fails to initiate the Shutdown Cooling (SDC)

Actions the same as event RHR-XHE-XM-ERROR.

3.10 BWR Specific Human Error Modeling Assumptions

☐ ***Containment venting*** causes loss of injection with suction on suppression pool. (Some exceptions in BWR 5/6 plants.)

☐ ***Suppression pool cooling*** failure force early depressurization (loss of HPCI/RCIC).

☐ ***Stuck-open relief valve*** events included in inadvertent-open relief valve event tree. (Station blackout sequences include explicit modeling of stuck-open relief valves.)

☐ ***Containment*** and equipment failure due to containment heatup rates based on existing generic thermal hydraulic analysis.[7]

(Technical issue pending resolution)

☐ ***Containment*** failure may cause loss of all injection (thermal-hydraulic issue). Credit for injection following containment failure is given if it is credited in the licensee PRA model.

(Technical issue pending resolution)

3.11 PWR Specific Human Error Modeling Assumptions

☐ ***Feed and bleed*** success allows time to recover steam generator cooling.

☐ ***Feed and bleed*** success requires two pressurizer power-operated relief valves (PORVs) (thermal-hydraulic issue; some plant PRAs require only one).

(Technical issue pending resolution)

☐ ***Small LOCA*** sequences (small LOCA or reactor coolant pump seal LOCA events) may not credit refueling water storage tank refill capability to preclude sump recirculation (thermal-hydraulic issue).

(Technical issue pending resolution)

7. Key recovery time estimates used in SPAR models are:

- One SRV open & HPCI or RCIC success: 4 hour recovery (Table 9.2, NUREG/CR-2182)
- High-pressure core spray success: 24 hour recovery (NUREG/CR-4550, Vol. 6, Rev. 1, Part 1)
- Other injection success: 10 hour recovery (NUREG/CR-3226, Peach Bottom IPE, Table 3.1.2.1.5-1)

☐ ***Small LOCA*** sequences (small LOCA or reactor coolant pump seal LOCA events) may not credit residual heat removal in PWRs with ice condenser containments. [8]

(Technical issue pending resolution)

3.12 General Event Tree Assumptions

The following general assumptions apply to both BWRs and PWRs. Specific BWR and PWR assumptions are identified.

☐ **Mission times.** A 24-hour mission time for all components to operate is assumed for success.

☐ **Instrumentation and control** not explicitly modeled (implicit in data). However, key I&C components are being addressed as part of the detailed PRA cut set level review. Addition of detailed instrumentation logic is impractical and not being added to the SPAR models due to the complex nature of the logic and the lack of detailed plant information. Additional level of detail in the electric power logic is being added to the SPAR models.

☐ **Common-cause failure** is not modeled across systems. (This issue is currently under reevaluation.)

☐ **Emergency diesel generators** are typically modeled with a 24 hour mission time.

☐ **Battery depletion.** Failure to recover ac power before the station batteries are depleted during a station blackout event will result in core damage. The key assumption here is that the loss of power to instrumentation and circuit breaker control would make it extremely difficult for recovery after battery depletion. Criteria for crediting recovery of offsite power beyond depletion of the divisional batteries are being developed. An outline of these criteria was presented at the April 2006 SRA counterpart meeting. At this meeting it was decided to leave criteria and models as is and to give credit for recovery as applicable on a case by case basis.

☐ **Operator errors.** Operator failure to operate a system within control parameters is only included if there are known failure modes caused by inadequate operator control of the system [e.g., high-pressure coolant injection (HPCI) failure resulting from multiple restarts if level is not controlled between the high and low level interlocks].

8. Thermal-hydraulic issue is whether a small LOCA actuates containment spray and empties the refueling water storage tank, thus requiring sump recirculation.

- **Pre-accident human errors**, such as miscalibration, misalignment, etc. are included as an element of demand failure probabilities (e.g., a pump fails to start event) – future implementation.

- **Small diversion paths.** Small diversion paths such as sample lines, small relief valves, vent lines, etc. that are smaller than one-third diameter of the main flowpath or have a flow-limiting orifice are not modeled. - future implementation.

- **Full-flow test line isolation valve failures** are included in the pump supercomponent as a mechanism for failing the pump (when system configuration allows).

- **Common-cause failures.** Common cause failures are modeled for active components only, except for plugging of heat exchangers. Common cause failure is only modeled for like components within a system, and not across system boundaries. Common cause is modeled for the following: motor-operated valves, air-operated valves, explosive valves, boiling water reactor (BWR) safety relief valves, pressurized water reactor (PWR) power-operated relief valve (PORV), check valves, pumps, heat exchangers and diesel generators.

- **Tank inventory.** Tanks are assumed to be filled to the minimum required by technical specifications. This amount is assumed to be sufficient for the required mission time, unless other information is available. For the refueling water storage tank (RWST) or equivalent, the assumption is that there is sufficient water for the injection phase.

- **Manual valves.** In general, manual valves that are not expected to be operated are typically not modeled. Manual valves that must change position are modeled; however, failure is dominated by human error.

- **Valves.** Valve failure basic events include the valve body, the driver, local I&C circuitry (mounted on or near the valve), and limit switches. Valve rupture is not modeled (except ISLOCA events). Plugging of valves and valve/stem separation are not generally modeled. Exceptions include valves in “dirty” systems (e.g., systems which take suction from external sources), valves known to have an interval between flow tests of several years or more, and, based on engineering judgment, valves that may be in a key location that can fail multiple trains or systems.

- **Heat exchangers.** Heat exchanger (usually decay heat removal heat exchangers) plugging events are generally included. By-pass lines around heat exchangers are modeled for the cooling function but are not considered for injection purposes.

- **Pumps.** Pump failure basic events include the pump body, the driver, the controller and local I&C circuitry, and any local self-contained cooling or lubricating systems.

☐ **Diesel generators.** Diesel generator basic events include all contributions to failures to start or run. These include all support systems unique to the diesel generator.

☐ **Containment sump (PWR) and suppression pool strainer (BWR)** plugging probabilities are based on generic values (GSI 191 issue). Awaiting industry implementation of GSI 191. SPAR issue resolution will reflect licensee's implementation of GSI 191 based on initiator-specific operator actions and failure (clogging) probability of new installed sump screens (passive/active). "Downstream effects" will be considered to the extent possible based on available information.

☐ **All initiators found in the PRA** with individual contributions greater than 1% of the internal events core damage frequency (CDF) are being added to the SPAR models.

☐ **Excessive LOCA event tree** with initiator frequency of 1E-7/year is being added to each SPAR model. Addressed as part of the detailed PRA cut set level review.

3.13 BWR Event Tree Modeling Assumptions

The following are typical modeling assumptions. Refer to the SPAR model manual for plant-specific assumptions.

☐ **CST inventory.** Condensate is credited as a makeup source in transients with up to and including 1 open SRV as well as in small LOCAs due to assumed sufficient hotwell makeup capability.CST inventory.

- Condensate (CDS) injection requires hotwell inventory plus makeup from the Condensate Storage Tank (CST) via the vacuum drag or condensate transfer pump operation.
- CST inventory is generally sufficient for high pressure coolant injection (HPCI), RCIC, control rod drive (CRD) missions but in some cases may required CST refill.

☐ **Steam supply with SORV.** The reactor core isolation cooling (RCIC) and high-pressure coolant injection (HPCI) systems will fail on low steam pressure and require alternate injection if there is a small LOCA or a stuck open relief valve (SORV). The failure may occur as soon as 1-2 hours after the system demand, but possibly much later.

☐ **HPCI/HPCS/RCIC suction swapover.** HPCI/high-pressure core spray (HPCS) will eventually switch suction from the CST to the suppression pool.

The operators will not be able to switch HPCI/HPCS and RCIC suction back to the CST once suction has transferred to the suppression pool.

Transfer of suction to the suppression pool may occur as a result of CST depletion, in which case transfer back would fail the system.

Transfer of suction before CST depletion may also occur because of high suppression pool level. In this case transfer back to the CST would require defeating automatic interlocks. Overriding the interlocks and transferring suction back to the CST in this case will be credited when procedural guidance is available

Station Blackout (SBO) sequences may have procedures that direct suction be maintained on the CST. If so, this will be modeled and will require CST refill for extended missions (beyond battery depletion).

☐ **ECCS dependency on room cooling.** Some models do not include the room cooling dependency for emergency core cooling systems (ECCS), such as RCIC and HPCI, based on recent licensee's analyses that proved room cooling is not needed.

☐ **High pool temperature and pressure.** Alternate injection will be required, following HPCI/RCIC success, if suppression pool cooling and shutdown cooling fail.

If RCIC is aligned to the suppression pool it will fail when the suppression pool temperature reaches approximately 173 F (newer plants 210 F to 265^{o}F) due to inadequate net positive suction head (NPSH).

If aligned to the CST, RCIC will eventually fail due to high exhaust backpressure (~25psig).

No credit is given for restarting RCIC following successful containment venting if/when the back pressure interlocks clear.

During a station blackout, power is not available to swap suction from the CST. Therefore, RCIC failure due to high suppression pool heatup is not assumed to occur.

☐ **Adequate NPSH** following containment cooling, sprays, or venting – low pressure.

Suppression pool cooling failure requires early depressurization (loss of HPCI/RCIC).

Containment venting causes loss of injection with suction on suppression pool.

The low-pressure coolant injection (LPCI) and core spray pumps will fail from lack of NPSH following containment venting, but will operate following success of containment sprays.

☐ **Containment failure.** Containment failure results in the loss of all injection and leads directly to core damage. Generally, no credit is given for a convenient containment failure location that would allow the continued operation of injection. However, credit may be considered as part of the detailed PRA cut set level review, if justification is considered sufficient, credit up to that permitted by the PRA is being incorporated into the SPAR models. The basic event CFAILED is used to model injection following containment failure in most models.

☐ **Vapor suppression system (VSS) failure** was not included in the SPAR model based on the conclusions from the NUREG-1150 studies and based on common practice in individual plant examinations (IPEs) submitted for BWR 5 and 6 plants. The most probable VSS failure appears to be stuck-open wetwell/drywell vacuum breakers, or structural failure of the suppression pool. These failure modes are considered extremely unlikely compared to the

unavailabilities of other front-line safety systems and are therefore excluded from the SPAR model.

☐ **Shutdown cooling (SDC) with SORV or LOCA.** Shutdown cooling (SDC) is not credited in cases where there is a breach in the reactor coolant system (either a break or a stuck open relief valve). Containment heating by the reactor coolant discharge is assumed to require success of suppression pool cooling, containment sprays, or containment venting to maintain injection in the long-term. This is a conservative assumption with respect to small breach situations, but correct for larger breaches.

☐ **CRD injection.** Control Rod Drive (CRD) injection is credited:

Early only for transients with no breaches (and if credited in the licensee PRA)

Late only for transients with no more than 1 SORV

Never in LOCA cases due to the uncertainty about sufficient makeup capability.

☐ **Battery depletion.** Failure to recover AC power before the station batteries are depleted during a station blackout event will result in core damage. Credit for ac power recovery after battery depletion is given only if the licensee PRA meets the Electric Power Research Institute (EPRI) guidelines.

☐ **PCS availability and SRV demands.** In cases where the power conversion system (PCS) remains available following an initiator, it is assumed there will be no safety relief valve (SRV) demands except in the case of ATWS.

In cases where the PCS is not available following the initiator, it is assumed that an adequate number of SRVs will open to relieve the resulting pressure transient. This is based on a small number of the available valves being required to protect against the pressure transient.

In the case of ATWS, relief valve opening is modeled explicitly because a large number of valves will be required to provide adequate pressure relief.

☐ **Stuck-open relief valve events** are included in inadvertent-open relief valve event tree.

☐ **Credit for Reactor Core Isolation Cooling (RCIC)** as a Source of Depressurization Equivalent to an Automatic Depressurization System (ADS) Valve. (thermal-hydraulic considerations) Addressed as part of the detailed PRA cut set level review. Earlier versions of SPAR models conservatively assumed that RCIC was unable to maintain core cooling during an Inadvertent Open Relief Valve (IORV) event until low-pressure injection sources could inject. This is at odds with NUREG/CR-4550 and industry thermal hydraulic analyses. Currently a small number of models still retain this conservative logic. This logic is being updated during the detailed PRA cut set level reviews. The Brunswick SPAR model will not be modified since the Brunswick PRA does not credit this scenario.

3.14 PWR Event Tree Modeling Assumptions

The following are typical SPAR modeling assumptions. Refer to the SPAR model manual for plant-specific assumptions.

- **Mission times.** A 24-hour mission time for all components to operate is assumed for success.

- **ATWS.** The failed reactor trip is modeled by transferring to the anticipated transient without scram (ATWS) event tree.

- **CST inventory.** The condensate storage tank (CST) will provide sufficient water so that providing a backup supply of water to the auxiliary feedwater pumps is not modeled.

- **Steam supply.** For all events, it is assumed there will be sufficient steam supply to operate the turbine driven auxiliary feedwater pump for the mission time.

- **RWST inventory.** For all of the loss-of-coolant accident (LOCA) sequences, the refueling water storage tank (RWST) is maintained at a level to satisfy early injection success without having to be refilled in order to supply enough water to the containment sump for recirculation.

- **Recovery of AC power.** The operator action to recover power in the station blackout event tree given a seal LOCA assumes that only offsite power is recovered.

  Assuming that only offsite power is recovered eliminates the need to model train dependent power recovery.

  If the recovery of the diesel generators were allowed, then the modeling of power to the front line components would have to take into account that only one train of power may be available for mitigation.

- **Battery depletion.** Failure to recover ac power before the station batteries are depleted during a station blackout event will result in core damage. The key assumption here is that the loss of power to instrumentation and circuit breaker control would make it extremely difficult for operator recovery after battery depletion. Recovery is allowed on a case by case basis if the licensee PRA meets the requirements of EPRI LOOP/SBO modeling guidelines.

- **Feed and bleed.** The PORV block valves are dependent upon ac power if they are closed during full power. Feed and bleed success allows time to recover steam generator cooling.

☐ **Small LOCA sequences** (SLOCA or RCP seal LOCA events) may not credit RWST refill capability to preclude sump recirculation (thermal-hydraulic issue).

☐ **Small LOCA sequences** (SLOCA or RCP seal LOCA events) may not credit RHR during in PWRs with ice condenser containments (Thermal-hydraulic issue is whether a SLOCA actuates containment spray and empties the RWST, thus requiring sump recirculation).

☐ **RCP Seal LOCA.** RCP seal failure logic and values per WOG 2000 have been incorporated into all SPAR models of Westinghouse plants. RCP seal failure logic and values per draft WCAP-16175-P (per NRC direction) have been incorporated into all SPAR models of Combustion Engineering (CE) plants. Babcock & Wilcox plant models incorporate either the approved Westinghouse model or the CE model.

☐ **SGTR.** Addressed as part of the detailed PRA cut set level review. Updated SGTR event tree logic is being added to all Westinghouse and Combustion Engineering SPAR models. Some additional refinement of the SGTR event tree is anticipated following resolution of issues related to reactor water storage tank (RWST) refill.

☐ **The Transient event tree** is being segregated into Loss of Condenser Heat (LOCHS), Loss of Main Feedwater (LOMFW) and Transient with power conversion system available. Addressed as part of the detailed PRA cut set level review.

SPAR Model Reviews: References	Section 4
	Rev. 2

4.0 References

Accepted methods, instructions, and modeling tips used to modify a SPAR model are listed below.

4.1 Event and Fault Trees

1. U.S. Nuclear Regulatory Commission, “Fault Tree handbook,” NUREG-0492, January 1981. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0492

2. U.S. Nuclear Regulatory Commission, “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Vol. 4 Tutorial,” NUREG/CR-6952, August 2008.

3. U.S. Nuclear Regulatory Commission, “PRA Procedures Guide,” NUREG/CR-2300, January 1983.

4. U.S. Nuclear Regulatory Commission, “PRA Review Manual,” NUREG/CR-3485, September 1985.

5. AEOD/S97-02, “Reactor Core Isolation Cooling System Reliability,” Idaho National Engineering and Environmental Laboratory, INEL-95/0196, Lockheed Martin June 1997.

4.2 Databases

1. U.S. Nuclear Regulatory Commission, “Reactor Operational Experience Results and Databases,” http://nrcoe.inel.gov/results/, August 2007.

2. U.S. Nuclear Regulatory Commission, “LER Search System,” https://nrcoe.inel.gov/secure/lersearch/index.cfm, August 2007. *(NRC internal Web site - available to NRC staff only)*

3. INPO, “Equipment Performance and Information Exchange (EPIX),” On-Line Database Available to NRC Staff Only.

4. U.S. Nuclear Regulatory Commission, “Event Reporting Guidelines 10 CFR 50.72 and 50.73,” NUREG-1022, Revision 2, October 2000.

5. U.S. Nuclear Regulatory Commission, “Reliability and Availability Data System (RADS),” Database Available in CD Format to NRC Staff Only.

6. U.S. Nuclear Regulatory Commission, “Common Cause Failure Data Base,” Database Available in CD Format to NRC Staff Only.

7. U.S. Nuclear Regulatory Commission, “Accident Sequence Precursor Database,” https://nrcoe.inel.gov/secure/aspdb/, August 2007. *(NRC internal Web site - available to NRC staff only)*

4.3 Parameter Estimation: Results

1. U.S. Nuclear Regulatory Commission, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants,” NUREG/CR-6928, February 2007. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6928/

2. U.S. Nuclear Regulatory Commission, “CCF Parameter Estimations, 2003 Update,” http://nrcoe.inl.gov/results/CCF/ParamEst2003/ccfparamest.htm, May 2006.

4.4 Parameter Estimation: Calculators

1. U.S. Nuclear Regulatory Commission, “Reliability and Availability Data System (RADS),” Database Available in CD Format to NRC Staff Only.

4.5 Parameter Estimation: Methods

1. U.S. Nuclear Regulatory Commission, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants,” NUREG/CR-6928, February 2007. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6928/

2. U.S. Nuclear Regulatory Commission, “Handbook of Parameter Estimation for Probabilistic Risk Assessment, NUREG/CR-6823,” September 2003.

   http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6823/

3. U.S. Nuclear Regulatory Commission, “Common-Cause Failure Database and Analysis System: Event Collection, Classification, and Coding,” NUREG/CR-6268, Draft.

4. U.S. Nuclear Regulatory Commission, “Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment,” NUREG/CR-5485, November 1998.

5. U.S. Nuclear Regulatory Commission, “Reevaluation of Station Blackout Risk at Nuclear Power Plants - Analysis of Loss of Offsite Power Events: 1986-2004,” NUREG/CR-6890, Volume 1, December 2005.

http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6890/

6. U.S. Nuclear Regulatory Commission, “Reevaluation of Station Blackout Risk at Nuclear Power Plants - Analysis of Loss of Station Blackout Risk,” NUREG/CR-6890, Volume 2, December 2005. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6890/

7. U.S. Nuclear Regulatory Commission, “Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995,” NUREG/CR-5750, February 1999. (Note: Refer to Appendix E for a methodology for time-trend analysis for initiating events accepted by the AMSE PRA standard.)

4.6 Human Reliability Analysis

1. U.S. Nuclear Regulatory Commission, “The SPAR-H Human Reliability Analysis Method,” NUREG/CR-6883, August 2005.

http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6883/

4.7 General References

1. American Society of Mechanical Engineers, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME RA-S-2005, 2005. [9]

2. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” Revision 1, January 2007.

http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-200/01-200r1.pdf

9 ASME PRA Standard is available through the NRC Library subscription access to codes and standards under “HIS Code and Standard, http://www.internal.nrc.gov/IRM/LIBRARY/standards/ihs.htm.”