Risk Assessment of Operational Events

Handbook

Volume 1 – Internal Events

Exposure Time Modeling – Failure Modeling
Mission Time Modeling – Common-Cause Failure Modeling – Recovery Modeling
Multi-Unit Considerations – Initiating Event Analysis – Human Reliability Analysis – Loss of Offsite Power Initiating Events – Support Systems Initiating Events - Analysis Road Map

UNITED STATES NUCLEAR REGULATORY COMMISSION

Revision 2.02

December 2017

SDP Phase 3 • ASP • MD 8.3

This page intentionally left blank.

TABLE OF CONTENTS

ACRONYMS

AC	alternating current
AFW	auxiliary feedwater
ASP	Accident Sequence Precursor (Program)
BOP	balance-of-plant
BWR	boiling-water reactor
CCF	common-cause failure
CCCG	common-cause component group
CCW	component cooling water
CDF	core damage frequency
CDP	core damage probability
CCDP	conditional core damage probability
DC	direct current
ECA	event and condition assessment
EDG	emergency diesel generator
EFW	emergency feedwater
EOP	emergency operating procedure
FTR	failure to run
FTS	failure to start
gpm	gallons per minute
HEP	human error probability
HFE	human failure event
HRA	human reliability analysis
IA	instrument air
ICES	Institute for Nuclear Power Operations Consolidated Events Database
IMC	Inspection Manual Chapter
LER	licensee event report
LOCA	loss-of-coolant accident
LOIA	loss of instrument air
LOOP	loss of offsite power
LPI	low-pressure injection
MD	management directive
MFW	main feedwater
NPSH	net positive suction head
NR	nonrecovery
PCS	power conversion system
PD	performance deficiency
PI	performance indicator

PORV	power-operated relief valve
PRA	probabilistic risk assessment
PSF	performance shaping factor
PWR	pressurized-water reactor
RADS	Reliability and Availability Data System
RASP	Risk Assessment Standardization Project
RCIC	reactor core isolation cooling
RHR	residual heat removal
ROP	Reactor Oversight Process
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SBO	station blackout
SDP	Significance Determination Process
SPAR (model)	standardized plant analysis risk (model)
SRA	senior reactor analyst
SRV	safety relief valve
SSC	structures, systems and/or components
SSU	safety systems unavailability
SW	service water
T/M	test or maintenance
TS	technical specifications

1.0 Introduction

1.1 Objectives

The first objective of the Risk Assessment of Operational Events Handbook (sometimes known as "RASP Handbook" or "handbook") is to document methods and guidance that NRC staff should use to achieve more consistent results when performing risk assessments of operational events and licensee performance issues.

The second objective is to provide analysts and standardized plant analysis risk (SPAR) model developers with additional guidance 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 the analyses. The individual plant SPAR models represent plant design and operation to a sufficient level for analyses, and include the current best industry average performance information.

This handbook represents best practices based on feedback and experience from the analyses of over 600 precursors of events dating back to 1969 in the Accident Sequence Precursor (ASP) Program and numerous Significance Determination Process (SDP) Phase 3 analyses (since 2000).

1.2 Scope of the Handbook

The scope of the handbook is provided below.

- ***Applications.*** The methods and processes described in the handbook can be primarily applied to risk assessments for Phase 3 of the SDP, the ASP Program, and event assessments under the NRC's Incident Investigation Program [in accordance with Management Directive (MD) 8.3, "NRC Incident Investigation Program"]. Collectively, these analyses are called event and condition assessments (ECAs) in this handbook. The guidance for the use of SPAR models and Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) software package can be applied in the risk analyses for other regulatory applications, such as the Generic Safety Issues Program and special risk studies of operational experience.

- ***Relationships to Program Requirements.*** This handbook is intended to provide guidance for implementing requirements contained in program-specific procedures, such as Inspection Manual Chapter (IMC) 0609, "Significance Determination Process," MD 8.3, IMC 0308, "Reactor Oversight Process Basis Document," and IMC 0309, "Reactive Inspection Decision Basis for Reactors." It is not the scope of this handbook to repeat program-specific requirements in the handbook, since these requirements may differ among applications and may change as programs evolve. Program-specific requirements supersede guidance in this handbook.

- ***Deviations from Methods and Guidance.*** Some unique events may require an enhancement of an existing method or development of new guidance. Deviations from methods and guidance in this handbook may be necessary for the analysis of atypical events. However, such deviations should be adequately documented in the analysis to allow for the ease of peer review. Changes in methodologies and guidance will be reflected in future revisions of this handbook.

1.3 Audience for the Handbook

The principal users of this handbook are senior reactor analysts (SRAs) and headquarters risk analysts involved with event and condition assessments. It is assumed that the analysts using this handbook have received probabilistic risk assessment (PRA) training at the SRA qualification level. Analysts using this handbook should be familiar with the event and condition assessments, SAPHIRE software package, and key SPAR model assumptions and technical issues. Although, this handbook could be used as a training guide, it is assumed that an analyst either has completed the series of NRC training courses in PRA, including "Risk Assessment in Event Evaluation," or has related experience.

1.4 Handbook Content

The revised handbook includes four volumes, designed to address Internal Events (Volume 1), External Events (Volume 2), SPAR Model Reviews (Volume 3), and Shutdown Events (Volume 4). The scope of these volumes is as follows:

- ***Volume 1, Internal Events.*** Volume 1, "Internal Events," provides generic methods and processes to estimate the risk significance of initiating events (e.g., reactor trips, losses of offsite power) and degraded conditions (e.g., a failed high-pressure injection pump, failed emergency power system) that have occurred at nuclear power plants.[1]

  Specifically, this volume provides guidance on the following analysis methods:

  – Exposure Time Modeling

  – Failure Modeling

  – Mission Time Modeling

  – Common-Cause Failure Modeling

  – Modeling Recovery and Repair Actions

  – Multi-Unit Considerations

  – Initiating Event Analyses

  – Human Reliability Analysis

  – Loss of Offsite Power Event Analysis

  – Support System Initiating Events

  Appendix A, "Road Map for Risk Analysis of Operational Events," provides a general overview on the risk analysis of initiating events and conditions in event assessment.

[1] In this handbook, "initiating event" and "degraded condition" are used to distinguish an incident involving a reactor trip demand from a loss of functionality during which no trip demand occurred. The terms "operational event" and "event," when used, refer to either an initiating event or a degraded condition.

Although, the guidance in this volume of the handbook focuses on the analysis of internal events during at-power operations, the basic processes for the risk analysis of initiating events and degraded conditions can be applied to external events, as well as events occurring during shutdown operations.

- ***Volume 2, External Events.*** Volume 2, "External Events," provides methods and guidance for the risk analysis of initiating events and conditions associated with external events. External events include internal flooding, internal fire, seismic, external flooding, external fire, high winds, tornado, hurricane, and others. This volume is intended to complement Volume 1 for Internal Events.

  Specifically, this volume provides the following guidance:

  – Internal Flood Modeling and Risk Quantification

  – Internal Fire Modeling and Risk Quantification

  – Seismic Event Modeling and Seismic Risk Quantification

  – Other External Events Modeling and Risk Quantification

- ***Volume 3, SPAR Model Reviews.*** Volume 3, "SPAR Model Reviews," provides analysts and SPAR model developers with additional guidance 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 the analyses. This volume provides checklists that can be used following modifications to SPAR models that are used to perform risk analysis of operational events. These checklists were based on the NUREG/CR-3485, "PRA Review Manual," American Society of Mechanical Engineers (ASME) RA-Sa-2009, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," and Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities, and experiences and lessons learned from SDP and ASP analyses.

  In addition, this volume summarizes key assumptions in a SPAR model and unresolved technical issues that may produce 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.

- ***Volume 4, Shutdown Events.*** Volume 4, "Shutdown Events," provides methods and practical guidance for modeling shutdown scenarios and quantifying their core damage frequency using SPAR models and SAPHIRE software. The current scope includes the following plant operating states for boiling-water reactors (BWRs) and pressurized-water reactors (PWRs): hot shutdown, cold shutdown, refueling outage, and mid-loop operations for PWRs.

1.5 Companion References to the Handbook

- ***References.*** Guidance in the four volumes of the handbook often refers to other references, as applicable to the application. Key companion references that are an extension to this handbook include:

  – PRA Standard (ASME RA-Sa-2009 and Regulatory Guide 1.200)

- NUREG/CR-6823, “Handbook of Parameter Estimation for Probabilistic Risk Assessment”
- NUREG-1792, “Good Practices for Implementing Human Reliability Analysis”
- NUREG-1842, “Evaluation of Human Reliability Analysis Methods Against Good Practices”
- NUREG/CR-6883,”SPAR-H Human Reliability Analysis Method”
- NUREG-1624, “Technical Basis and Implementation Guide for a Technique for Human Event Analysis”
- NUREG-1880, “ATHEANA User’s Guide”
- NUREG/CR-6850, “EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Volume 2: Detailed Methodology”
- Handbook for Phase 3 Fire Protection SDP Analysis
- SAPHIRE 8 User Manuals (NUREG/CR-7039, Volumes 1–7)
- INL/EXT-10-18533, “SPAR-H Step-by-Step Guidance”
- NUREG/CR-6890, “Reevaluation of Station Blackout Risk at Nuclear Power Plants”
- Plant-specific SPAR model manual

1.6 Future Updates to the Handbook

It is intended that this handbook will be updated on a periodic and as-needed basis, based on user comments and insights gained from “field application” of the document. New topics will also be added as needed, and the handbook can also be re-configured and/or reformatted based on user suggestions.

1.7 Questions, Comments, and Suggestions

Questions, comments, and suggestions should be directed to the following:

Internal NRC staff and NRC contractors should contact:

- Volume 1, Internal Events
  - Christopher Hunter, 301-415-1394, Christopher.Hunter@nrc.gov
  - Michael Montecalvo, 301-415-1678, Michael.Montecalvo@nrc.gov
  - Don Marksberry, 301-415-1543, Don.Marksberry@nrc.gov

- Volume 2, External Events and Volume 4, Shutdown Events
  - Selim Sancaktar, 301-415-2391, Selim.Sancaktar@nrc.gov
  - Ching Ng, 301-415-8054, Ching.Ng@nrc.gov

- Volume 3, SPAR Model Reviews
  - Jeffery Wood, 301-415-0953, Jeffery.Wood@nrc.gov

External NRC stakeholders (e.g., public, licensees) should contact:

- All Handbook Volumes
  - Candace Spore, 301-415-8537, Candace.Spore@nrc.gov

This page intentionally left blank.

2.0 Exposure Time Modeling

2.1 Objective and Scope

This section provides guidance for adjusting the baseline exposure time (one year) in Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) to best reflect the duration period of the failed or degraded structure, system, or component (SSC) that was observed during the operational event. The exposure time (sometimes known as failure or condition duration) is used by the SAPHIRE code in a condition analysis to model the duration over which the risk of the condition (i.e., failure, degradation) is measured. After SAPHIRE completes the cut set evaluation, it will apply the exposure time of the failure or degradation. The estimation of exposure time for various conditions observed in operational events is discussed below. This section applies to a condition analysis as part of a Significance Determination Process (SDP), Accident Sequence Precursor (ASP), or Management Directive (MD) 8.3, "NRC Incident Investigation Program," assessment.

2.2 Definitions

- ***Exposure Time.***[2] Exposure time (*T*) is the duration period of the failed or degraded SSC being assessed that is reasonably known to have existed.
  - The repair time, if any, should be included in the exposure time.
  - Exposure time may be operating mode (i.e., power level) dependent, in which case the time during shutdown, for example, is not included in the exposure time, unless the component/system was required by technical specifications (TS) to be operable during shutdown.

- ***Repair Time.*** The probabilistic risk assessment (PRA) Standard defines repair time as "*. . . the period from identification of a component failure until it is returned to service.*"[3] No standard regulatory definition exists for the term "returned to service." Therefore, for the purpose of modeling exposure time in event and condition assessments, "returned to service" means the time at which any clearance tagging associated with the repair is removed and successful post-maintenance surveillance testing of the component has been completed to demonstrate performance of its safety function.[4]

  Some exceptions when repair time should not be included in the exposure time include the following:

[2] SAPHIRE uses the term "event duration time" (in hours) instead of exposure time.

[3] The PRA Standard referred in this handbook includes ASME/ANS RA-Sa-2009, as endorsed by Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities."

[4] In most cases, the period of time between the removal of clearance tagging and completion of required post-maintenance surveillance testing is only a few hours and should have negligible contribution to the exposure time. However, this period of time can be modeled separately with a recovery analysis for potentially risk-significant cases.

- For MD 8.3 assessments, if, at the time of the analysis, repairs are still ongoing and the plant is still at power, then repair time should not be included in the exposure time.
- If the plant is shutdown and the deficiency only affects an at-power condition, then repair time should not be included.
- If the repair involves a long time requiring design and construction (e.g., fire wall), and other mitigating actions were immediately taken (e.g., fire watch), then repair time may not be included. This is a judgment call, not a rule.

- ***t Period.*** The *t period* is the time between last successful functional operation and the unsuccessful functional operation or failure discovery date.
  - The last successful functional operation can include a surveillance test or unplanned demand.
  - The date of discovery is generally within the exposure time. However, if the component was determined to be degraded following repair, then the date of discovery is the date when the component was returned to service following the repair. The point is that the *t period* ends when the work began to change the component, even if the crew's discovery of the degraded condition had not yet occurred.

2.3 Exposure Time = t + Repair Time

- ***T = t + Repair Time.*** For a failure that was determined to have occurred when the component was last functionally operated in a test or unplanned demand (e.g., failure occurred when the component was being secured), the exposure time (*T*) is equal to the total time from the last successful operation to the unsuccessful operation (*t*) plus repair time.

- This exposure time determination approach is appropriate for standby or periodically operated components that fail due to a degradation mechanism that is not gradually affecting the component during the standby time period.

- The *t period* should be considered for the following cases:
  - *Known inception of failure.* The failure was determined to have occurred when the component was last functionally operated in a test or unplanned demand.
  - *Unknown inception of failure or no root cause assessment.* The failure mechanism was unknown and the root cause assessment was not sufficient or not complete to identify the cause of the failure.

- Repair time is added to the *t period*.

- Evidence for considering that a failure occurred during or immediately after last successful operation include the following:
  - Failure occurred due to human error as the component was being secured from the last test or operation.
  - Mechanical failure resulting in failure to start that could have only occurred when the component last operated or changed state.
  - Replacement part was defective, but passed initial operational test.

- An event (e.g., water hammer) that caused the failure of a component remained unnoticed until the next unsuccessful operation of the component.
- Pump fails to provide adequate discharge pressure after start due to foreign material entering the pump. The pump was successful during the last test. The debris existed in the tank for over a year. The debris was most likely in or near the suction line that it eventually clogged for the entire period since the last successful operation.

2.4 Exposure Time = t/2 + Repair Time

- ***T = t/2 + Repair Time.*** For a failure that could have occurred at any time since the component was last operated (e.g., time of actual failure cannot be determined due to the nature of the failure mechanism), the exposure time (*T*) is equal to one-half of the time period since the last successful functional operation of the component (*t/2*) plus repair time.

- This exposure time determination approach is appropriate for standby or periodically operated components that fail due to a degradation mechanism that gradually affects the component during the standby time period.

- The *t/2 period* should be considered for the following cases:
  - A thorough root cause assessment by knowledgeable resource experts ruled out failure occurring at the time of the last functional operation, but the inception of the failure after the last operation could not be determined after careful reviews.
  - A thorough root cause assessment by knowledgeable resource experts could not rule out the inception of the failure, but a failure mechanism and cause were reasonably known.

- Repair time is added to the *t/2 period*.

- Evidence for considering the failure occurred sometime *between* last successful operation and discovery time include the following:
  - There is no strong evidence that the cause of the failure was related to the last successful operation.
  - Failure mechanism was caused by nominal environmental conditions (e.g., corrosion, degradation of condensate storage tank floating diaphragm).

2.5 Exposure Time for Component Run Failures

- This exposure time determination approach is appropriate for standby or periodically operated components that fail due to a degradation mechanism that affects the component during its operation or run time (i.e., the degradation leading to failure occurs during operation, and is assumed to be linearly proportional to the run time). In addition, the degradation mechanism is basically dormant when the component is in standby. In both cases below, the exposure time starts at the time when the component no longer had the capability to operate for the PRA mission time (i.e., 24 hours).

- ***$\sum$(run times) > PRA Mission Time (24 hours), Inception Time Known or NOT Known.*** The exposure time starts at the time when the component no longer had the capability to operate for the 24-hour PRA mission time. This approach could be conservative if the unknown inception time of the degradation mechanism was actually after the calculated beginning of the exposure time.

Example A– Component accumulated 36 hours of run time during surveillance tests prior to run failure on September 30. Inception of failure mechanism was known to be January 1. Repair time is negligible. Exposure time is 6 months based on the 24 hours of run time (PRA mission time) prior to failure.[5]

Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours	4 hours
←Inception of condition			Failure to run occurs→					
			← Exposure Time (based on 24-hour PRA mission time)→					

- ***∑(run times) < PRA Mission Time (24 hours), Inception Time Known.*** When the inception of the condition is known and the accumulation run time between the time of inception and time of failure is less than the PRA mission time (24 hours), the exposure time should start at the time of inception and end when the repaired component was returned to service.[6]

Example B– Component accumulated only 9 hours of run time during surveillance tests between the known inception date and the date of failure on September 30. Repair time is negligible. Exposure time is 9 months.

Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
1 hour	1 hour	1 hour	1 hour	1 hour	1 hour	1 hour	1 hour	1 hour
←Inception of condition Failure to run occurs→								
←------------------- Exposure Time (based on 24-hour PRA mission time) ----------------------→								

- Repair time is included in the exposure time.

2.6 Exposure Time for Continuous Component Operation Failures

- For failure of a component that is normally in continuous operation while at-power (e.g., normally operating service water pump), the exposure time should be the PRA mission time (i.e., 24 hours).

- The analysis of some conditions may involve fault tree modeling of a support system initiating event. In this case, mission times for the normally running components may be more than 24 hours.

2.7 Maximum Exposure Time

The maximum exposure time (T) in a condition analysis is usually limited to one year; even though, the condition may have existed for longer than one year (e.g., design deficiency present since installation, modification, or construction).

2.8 Exposure Time for Multiple Conditions

- In SDP analyses, the risk significance of multiple conditions are only assessed if the described concurrent conditions were caused by the same performance deficiency (except for poor management or cross cutting programmatic issues).

[5] The 6 months exposure time would apply in this case even if the inception date was not known.

[6] For the case where the inception time is not known, the case "∑(run times) > PRA mission time (24 hours), inception time known or not known" would apply.

- This category includes the summation of exposure time segments of multiple equipment or functional degradations.

- The treatment of multiple conditions is specific to the analysis application. Refer to the program-specific procedure (i.e., SDP, ASP, and MD 8.3).

- Section 2.10 of this handbook provides examples of exposure times for multiple conditions.

2.9 Exposure Time for T/M Contribution

- This category includes the addition of an exposure time segments involving a failed/degraded component and a concurrent unavailability of a component in test or maintenance (T/M) due to an unrelated cause.

- For a component in test or maintenance where there is no prior knowledge that a failed condition existed in that component and where no failure was discovered in that component during testing and maintenance, assume an exposure time segment involving the component in test or maintenance equal to the time period that the component was tagged out-of-service.

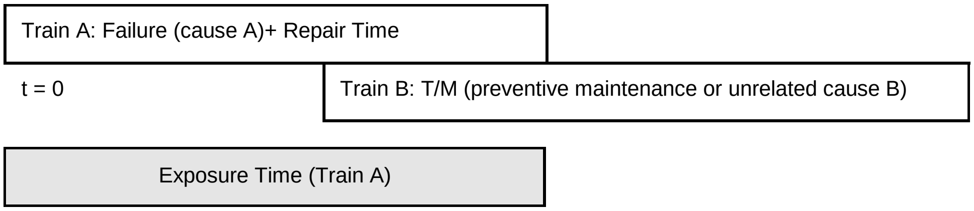
- The maintenance performed during shutdown is not included in the determination of component unavailability during power operation.

- If a scheduled T/M discovered a degraded condition, then include the T/M outage time, as well as the repair time, in the exposure time.

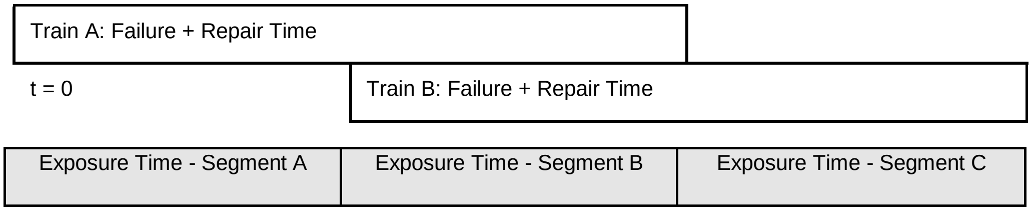
- Section 2.10 of this handbook provides examples of exposure times for T/M contributions.

2.10 Examples of Exposure Times for Multiple Conditions and T/M

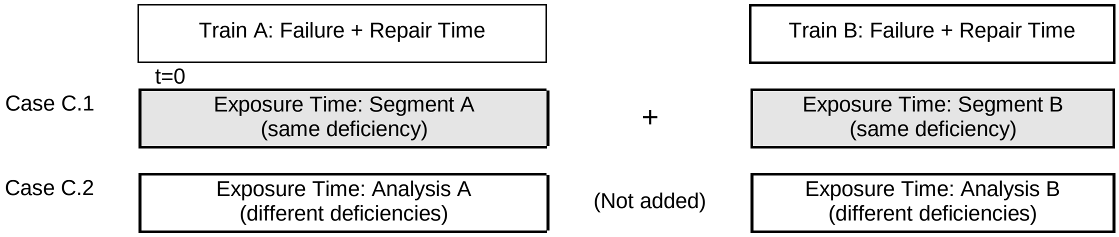
- ***Case A– Condition Analysis of One Failure.*** Failure of one train and unavailability of another train with overlapping exposure times:
  - If the cause of the T/M outage of Train B is not related to the performance deficiency (PD) that caused the failure of Train A, then the exposure time only applies to the Train A failure.


Train A: Failure (cause A)+ Repair Time
t = 0
Train B: T/M (preventive maintenance or unrelated cause B)
Exposure Time (Train A)

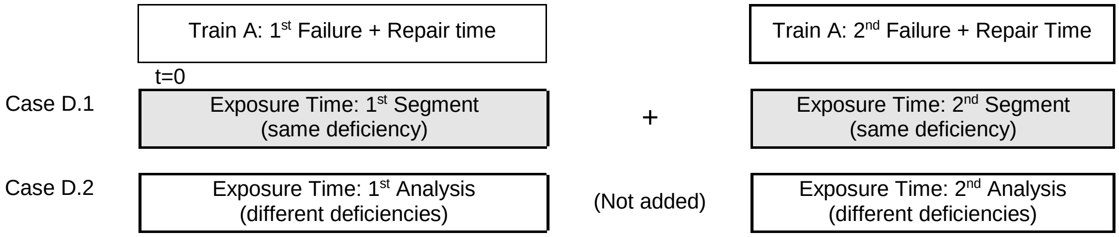
- ***Case B– Condition Analysis of Two Failures with Overlap.*** Failure of one train and a failure in another train with overlapping exposure times:
  - If both failures were related to the same PD *(applies to SDP and ASP analyses)* or if both failures are not related to the same PD *(applies to ASP analysis only)*, then the exposure time is the sum of the three segments.


Train A: Failure + Repair Time
t = 0
Train B: Failure + Repair Time
Exposure Time - Segment A
Exposure Time - Segment B
Exposure Time - Segment C

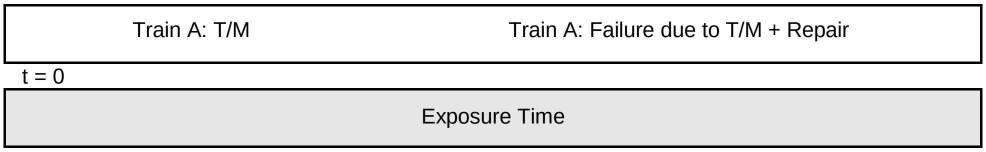
- ***Case C– Condition Analysis of Two Failures without Overlap.*** Failure of one train and a failure in another train with no overlapping exposure times:
  - *Case C.1.* If both failures were related to the same PD (other than poor management or cross-cutting programs), then the exposure time is the sum of the two segments *(applies to SDP and ASP analyses).*
  - *Case C.2.* If both failures are not related to the same PD, then each condition is analyzed separately *(applies to SDP and ASP analyses).*


Train A: Failure + Repair Time
Train B: Failure + Repair Time
t=0
Case C.1
Exposure Time: Segment A (same deficiency)
+
Exposure Time: Segment B (same deficiency)
Case C.2
Exposure Time: Analysis A (different deficiencies)
(Not added)
Exposure Time: Analysis B (different deficiencies)

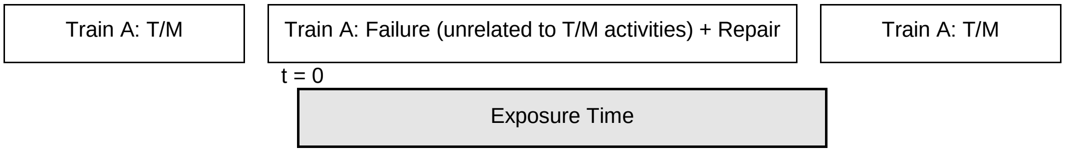
- ***Case D– Condition Analysis of Repeated Failures in the Same Train.*** Failure of a train and a second failure of the same train (after attempted repair of the first failure):
  - *Case D.1.* If both failures were related to the same PD (other than poor management or cross cutting programs), then the exposure time is the sum of the two segments *(applies to SDP and ASP analyses).*
  - *Case D.2.* If both failures are not related to the same PD, then each condition is analyzed separately *(applies to SDP and ASP analyses).*


Train A: 1st Failure + Repair time
Train A: 2nd Failure + Repair Time
t=0
Case D.1
Exposure Time: 1st Segment (same deficiency)
+
Exposure Time: 2nd Segment (same deficiency)
Case D.2
Exposure Time: 1st Analysis (different deficiencies)
(Not added)
Exposure Time: 2nd Analysis (different deficiencies)

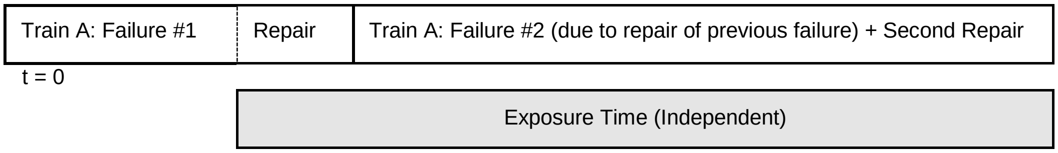
- ***Case E– Failure of a Train Caused by a Prior T/M Activity.***
  - If a component was not properly returned to service following a test or maintenance activity, then the exposure time includes the first maintenance outage time.



- ***Case F– Failure of a Train not Caused by T/M Activity.***
  - T/M outages not related to the failure are not included in the exposure time.



- ***Case G– Repeated Failures in Same Train, Later Failure Induced by Unrelated Cause.***
  - This case assumes that the causes of both failures are not related. If the repair of the first failure caused the second failure, then the exposure time of the second failure includes the repair time of the first failure.


Train A: Failure #1
Repair
Train A: Failure #2 (due to repair of previous failure) + Second Repair
t = 0
Exposure Time (Independent)

This page intentionally left blank.

3.0 Failure Modeling

3.1 Objective and Scope

This section provides guidance for the treatment of failures observed during an operational event. A failure of a structure, system, or component (SSC) is represented in the standardized plant analysis risk (SPAR) model by basic events based on failure modes (e.g., fail-to-start, fail-to-run, fail-to-open, and fail-to-close). The treatment of failures of varying severity in event and condition assessment (ECA) and the modeling of failures in SPAR models using the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) code are discussed below. This section applies to initiating event and condition analyses in Significance Determination Process (SDP), Accident Sequence Precursor (ASP), or Management Directive (MD) 8.3, "NRC Incident Investigation Program," assessments.

3.2 Treatment of Failures in ECA– General

Component malfunction events can be classified into one of the following three failure event severity categories as defined in Section 5.2 of NUREG/CR-6823, "Handbook of Parameter Estimation for Probabilistic Risk Assessment": (1) catastrophic failures, (2) degraded failures, and (3) incipient failures. The treatment of these failure categories in ECA are summarized below. Specific examples in ECA are provided in Section 3.3, below.

- ***Catastrophic Failures.***
  - Catastrophic failures require some kind of repair or replacement action on the component in order to restore the component to operability.
  - Catastrophic failures are generally modeled by setting the basic event to TRUE and setting its nonrecovery probability, if applicable, to TRUE.

- ***Degraded Failures.***[7]
  - Degraded failures can prevent a system or train from meeting the success criteria modeled in the probabilistic risk assessment (PRA) model.
  - Degraded failures of SSCs may result in a higher failure probability on demand (e.g., failure to start) or fail before completing its mission time (e.g., failure to run).
  - Degraded structures may fail from a more severe external event or fail at a condition outside its rated specifications (e.g., a fire wall rating).
  - Degraded failures are generally modeled by one of the following applications:
    - ○ Adjusting the failure probability to a higher value, based on appropriate engineering analysis, to reflect increased likelihood of failure (e.g., due to aging, growth of a crack).

[7] Per Supporting Requirement SY-A22 (Capability Category III) in the PRA Standard, no credit should be taken for component operability beyond its design or rated capabilities unless supported by an appropriate combination of test or operational data, engineering analysis, or expert judgment. This requirement applies to all components, not just degraded ones.

    - ○ Setting the basic event to its nonrecovery probability (based on a recovery analysis) when it is not feasible to conduct an engineering analysis to determine the impact of the degradation on the failure probability.
    - ○ Adjusting the PRA success criteria.

      For example, suppose that there is a degraded pump in a three-train system with a 1 out of 3 success criterion. If degradation reduces the pump's flow rate or head, it may be appropriate to use a 2 out of 3 success criterion to reflect the impact of the pump degradation.
    - ○ In some cases, refining the SPAR model to remove conservatism and thereby reducing the importance of the degradation.

- ***Incipient Failures.***
  - – Incipient failures have no significant degradation in performance but there are indications of a developing fault. An incipient failure that does not conform to its safety analysis basis may be classified as inoperable. The term "inoperable" has regulatory significance. It does not necessarily imply a state of physical failure. A component can be inoperable and still able to perform its PRA mitigation function over its assumed mission time.
  - – Although an incipient failure will typically lead to a corrective action, the corrective action may or may not make the component unavailable to perform its function.

    For example, maintenance on a motor operator of a normally open valve will not lead to the unavailability of the valve if the valve is required to be open for system operation (its designed safety function position) and remains open during the maintenance activity. This illustrates the importance of ascertaining from event records the modes of a component operation that a corrective action would prevent.

- ***Unknown Classification of Severity.***
  - – In the absence of sufficient information, the tendency is to conservatively model such events as catastrophic failures. This is reasonable as long as the impact on the analysis results is not significant. If the impact is significant, it is important to clearly state the assumptions when presenting the risk results.
  - – For cases where the judgment of the analyst is important to the analysis results, it could be incorporated explicitly into the analysis quantification as a source of uncertainty.

3.3 Treatment of Failures in ECA– Other Examples

Specific examples of the treatment of failure severity categories (defined above) are provided below.

- ***Catastrophic Failure during Tests.*** A failure to start or run during a test that closely mimics the conditions that the component would be subjected to during an unplanned demand should be modeled by adding the component failure mode in the fault tree, if it is not already there, and setting the corresponding basic event to TRUE.

- ***Degradation without Loss of Function (Incipient Failure).***
  - – A degraded failure that was not serious enough to prevent the component from performing its function should be treated as an incipient failure. The failure of the component should match the definition of the failure in the PRA model.

    For example, vibration in a pump that results in the pump only delivering 500 gallons per minute (gpm) instead of the rated flow of 600 gpm as required by the technical specifications (TS) is not a failure event given that 500 gpm is determined to be sufficient to meet its PRA functional success criteria for the PRA mission time.

  - If the degraded failure was revealed during a test of short duration, it may not be known whether the component would have succeeded over its mission time. In this case, an attempt can be made to extrapolate the rate of degradation to determine if the component would meet its failure criteria sometime during its mission time.

    For example, a pump develops a slow oil leak during a test. If the rate of leakage is such that the pump would run out of lubricating oil during the required pump mission time as modeled in the PRA, then the event is considered as a pump failure to continue to run.

  - An event reported as a "failure to meet TS," but which would not fail any PRA mission, should be treated as an incipient failure.

    For example, the failure of an emergency diesel generator (EDG) to start and pick up loads within 10 seconds might be a reportable failure for regulatory purposes, even if the loads were picked up in 20 seconds. However, in the PRA model, this is not a failure if the loads were picked up in time to mitigate the initiating events modeled.[8] However, this failure would require maintenance to alleviate the fast loading failure.

- ***Failure of Redundant Piece Part.*** An event involving a degraded or failed state of a redundant piece part may be excluded as a failure if the component boundary includes the redundant piece part as long as there is no impact on its ability to perform mitigation functions during the PRA mission time.

  For example, if a diesel generator has two redundant air start motors that are included in the diesel generator boundary definition (in the PRA model), failure of one air start motor would not be counted as a failure of the diesel generator. This example illustrates how a coarse definition of a component boundary can result in the failure to account for some degraded component states.

- ***Failure that could not be repeated during Tests.***

  - If a failure during a test could not be repeated on subsequent tries and the cause cannot be determined, then assume a recoverable failure over an appropriate exposure time, such as one surveillance test cycle.
  - A review of licensee event reports (LERs) and the Institute for Nuclear Power Operations Consolidated Events (ICES) database for similar spurious failures may reveal a chronic pattern. An update of the component failure probability may be warranted for repeated occurrences of spurious failures.
  - If a spurious failure occurred during an unplanned demand, then the basic event should be set to TRUE. Recovery may be appropriate since spurious failures are in many cases easily recoverable.

- ***Failure that Can Be Easily Recovered.*** A component failure that can be quickly recovered may be modeled in the PRA as a failure with recovery. Refer to Section 6 for details.

- ***Successive Failure of Same Component over Short Time Interval.***

  - Successive failures of the same component over a short time interval may be counted as a single failure, if the cause of the successive failures was due to improper maintenance to fix the initial problem. The exposure time should reflect the total time covered by the

[8] Loss of offsite power/loss-of-coolant accident scenarios for which the 10-second EDG start times are required may be screened out in most PRA models.

successive failures from the time of discovery of the first failure through the final recovery time.

  - Failure of a component during post-maintenance testing may be considered as a continuation of the original failure, if the cause of the test failure was related either to the maintenance activity or to the original failure that the maintenance was trying to correct. For SDP analyses, the cause of the failures should be related to the same performance deficiency.
  - Refer to Section 2 for details and exceptions.

- ***Failure to Run of a Standby Component.***
  - *Extended run failure.* A component that fails to run during an extended test (e.g., EDG 24-hour duration test) or under normal operation (e.g., motor-driven auxiliary feedwater pump during hot shutdown conditions) may not impact the mission time of many sequences modeled in the PRA.

    For example, an EDG that fails after 23 hours in a 24-hour duration test due to excessive wear in one cylinder liner may be able to carry out its mission for all sequences in the plant=s station blackout model, as long as the wear was time dependent and not randomly catastrophic.
  - *Short test failure.* A component that fails to run during a routine surveillance test may accumulate enough run time to satisfy the mission time of short-term sequences. A run failure may alternatively signal the presence of a condition that might have precluded success in longer-run-time missions for an appreciable exposure time. Refer to Section 2 for a discussion of this point.
  - A component that fails to run may indicate a gradual degradation with longer run time-before-failure at the beginning of the degradation. Evidence of time-dependent wear, such as metal shavings in the lubrication oil, may support a shorter exposure time for some PRA sequences with shorter mission times at the beginning of the degradation when success was possible because the degradation was not too advanced.
  - The rate of gradual degradation is often difficult to estimate. The degradation rate could be linear or exponential.

- ***Failure to Run of a Continuous Running Component.*** A failure of a component that runs continuously during at-power operations (e.g., service water pump) is typically more readily recoverable through use of redundant trains or alternate systems because of immediate detection. The potential for a plant trip due to an unsuccessful operator intervention may need to be considered (e.g., manual alignment of a standby train).

3.4 SPAR Models– Failure Mode Definitions

- ***Why Failure Mode Definitions Are Important in SPAR Models.*** If a basic event represents a failure of a pump to start, it usually means exactly that. However, it is not unusual in PRAs to define diesel generator fails to start as encompassing a failure to start or a failure during the first hour given that the start was successful. Whatever definitions are used, the failure event must be matched with the appropriate basic event.

- ***Where to Find Failure Mode Definitions Used in SPAR Models.***
  - Failure probabilities used in SPAR models are based on the analysis methods and results from NUREG/CR-6928, “Industry-Average Performance for Components and

Initiating Events at U.S. Commercial Nuclear Power Plants," Section 5 and Appendix A. The failure modes and component boundary definitions are also documented in Appendix A of NUREG/CR-6928. Updates to NUREG/CR-6928 will be posted on the Reactor Operational Experience Results and Databases Web page.[9]

  - Modeling limitations that exclude failure modes can be found in the fault tree section in the plant-specific SPAR model manual.

- ***Failure to Start Events in SPAR Models.***
  - Failures to start are typically modeled to occur prior to steady-state operation.
  - There is no explicit time frame (e.g., 30 minutes) associated with failures to start.

- ***Failure to Run Events in SPAR Models.***
  - For SSCs that are initially in standby, failures to run are usually subdivided into two bins. These bins consist of the first hour (early) of operation and greater than one hour (late).
  - Note: The binning of data may change in the future based on Bayesian analysis of future operating experience. Check the plant-specific SPAR model manuals and fault trees for the current modeling of failure to run parameters.

3.5 SAPHIRE Code– Modeling Failures

- ***Know Where the Basic Event Is Used in the SPAR Model.*** A basic event modification can adversely affect other parts of the SPAR model. Refer to Step 4 in Appendix A for considerations on this topic.

- ***Common-Cause Failure Analysis in Event Assessment.*** This activity involves the treatment of component failures and degradations and the common-cause failure (CCF) implications for the evaluation of the operational event. Refer to Section 5 for detailed guidance on this topic.

- ***Consideration of Success Terms in SAPHIRE.*** SAPHIRE normally uses a quantification method that only considers event tree failure branches. The success branches are not quantified. If adjusting a basic event to a higher probability results in an increase in event tree branch failure probability so that the success branch probability is significantly affected (reduced to something less than 0.95), then the success branch may have a significant impact on the results. Consult Idaho National Laboratory for guidance on incorporating success terms in the model results.

- ***Modeling a Support System Failure.***
  - If the support system is not included in the SPAR model, the impact of the failure on front line safety systems is addressed by setting the impacted components to TRUE in the "Current Case". CCF implications should be reviewed in accordance with Section 5.
  - The modeling of a support system failure recognizes that as long as the failure remains unrecovered, all impacted SSCs are unavailable; but if the support system failure is

[9] Failure modes used in the SPAR models were identified in the Office of Nuclear Regulatory Research system and component reliability studies. See the Reactor Operational Experience Results and Databases Web page for details. Data used to estimate failure probabilities are primarily from EPIX failure reports. The results were estimated using the RADS calculator. Analysis methods are documented in NUREG/CR-6823.

recovered, all impacted SSCs may be recoverable given that necessary operator actions are accounted.

  - Use of an event tree may be more appropriate for modeling support system failures when the operating experience data show likelihood of recovery as a function of time after failure.

    For example, cases of recovery of instrument air losses shortly after the reactor trip (usually resulting in a manual trip due to gradual closing of feed regulating valves) have been found in the operating experience. Air leaks are usually quickly detectable (due the noise, etc.) resulting in prompt action to bypass the leak to restore system pressure. The availability of more time means that lower nonrecovery probability can be modeled in top events of an event tree.

- ***Whether to Set the Basic Event to TRUE or 1.0 in SAPHIRE.***[10] The mapping of an observed failure in the SPAR model usually require the analyst to set the basic event to TRUE in SAPHIRE. Setting the basic event to 1.0 (also means failed) can result in differences in cut sets. Both choices have advantages and disadvantages as summarized below.
  - *Know where the basic event is used in the SPAR model.* A basic event modification can adversely affect other parts of the SPAR model. Refer to Step 4 in Appendix A for considerations on this topic.
  - *Setting the basic event to TRUE instead of 1.0*. The following adjustments will be performed by SAPHIRE when a basic event is set to TRUE:
    - Setting an event to TRUE actually changes the logic of the fault tree, pruning appropriate branches and basic events from the fault tree. Therefore, the affected fault trees will be resolved to generate new cut sets rather than just re-quantifying the existing cut sets with a new basic event failure probability.
    - Post-processing rules will not be applied to resulting sequence cut sets affected by the basic event that was set to TRUE, because the basic event was removed from the cut sets.[11] Illogical or mutually exclusive cut sets may be generated.
  - *Setting the basic event to 1.0 instead of TRUE.* The following adjustments will be performed by SAPHIRE when a basic event is set to 1.0:
    - The basic event will remain in the resulting sequence cut sets. This allows the analyst to review cut sets associated with a particular basic event of interest.
    - Setting the basic event to 1.0 can result in non-minimal cut sets. The cut sets should be inspected to see if they make sense. Non-minimal cut sets may need to be eliminated.
    - Post-processing will be applied to the resulting sequence cut sets. Post-processing rules will identify the basic event and operate accordingly.

[10] In both cases, the cut sets should be inspected to see if they make sense. Illogical risk-important cut sets may need to be eliminated. In addition, the analyst may have to modify post-processing rules to produce the correct cut sets.

[11] Post-processing rules were referred to as “recovery rules” in past version of SAPHIRE. These rules have evolved from the simple inclusion of recovery events in Revision 2 SPAR models into a powerful rule-based system for cut set manipulation.

4.0 Mission Time Modeling

4.1 Objective and Scope

This section provides guidance for adjusting the mission time (i.e., decrease or increase) of a structure, system, or component (SSC) from the baseline 24-hour mission time that is typically credited in standardized plant analysis risk (SPAR) models. The probabilistic risk assessment (PRA) Standard defines mission time as "*. . . the time period that a system or component is required to operate in order to successfully perform its function.*"[12] In the SPAR models, a 24-hour mission time is assumed for all sequences and most structures, systems, or components (SSCs). The supporting requirements in the PRA Standard suggest a minimum mission time of 24 hours. However, exceptions are permitted for shorter and longer mission times for certain situations, as discussed below. Considerations for adjusting mission times in SPAR models for event and condition assessments (ECA) using the SAPHIRE code are also discussed. This section applies to initiating event and condition analyses in Significance Determination Process (SDP), Accident Sequence Precursor (ASP), or Management Directive (MD) 8.3, "NRC Incident Investigation Program," assessments.

4.2 Treatment of Mission Time in ECA– General Considerations

- The SPAR models assume a 24-hour mission time for all sequences and most SSCs. Guidance for adjusting the mission time for a sequence and/or SSC in an ECA should follow the supporting requirements from the PRA Standard. Supporting requirements for specifying an appropriate mission time for the modeled accident sequences, support systems, and intersystem/intrasystem dependencies are provided in the Section 4.9.

- A component or system mission time is 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.

- Mission time modifications should be made to the base case SPAR model. As with all modifications to a SPAR model, consult Idaho National Laboratory before or after making the model modification. Checklists to guide the review of SPAR model modifications are provided in Volume 3 of this handbook.

- These considerations apply to individual basic events, and may also apply to classes of basic events sharing the same mission time requirement.

4.3 Decreasing Mission Time (< 24 Hours)

- Mission time less than 24 hours may be appropriate for certain sequences. Mission times for individual SSCs that function during the accident sequence may be less than 24 hours, as long as an appropriate set of systems, components, and operator actions are modeled to

[12] The PRA Standard referred in this handbook includes ASME/ANS RA-Sa-2009, as endorsed by Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities."

support the full sequence mission time.

Considerations for decreasing the mission time of a SSC may include:

- SSC mission time may be sequence or cut set dependent.
- Decreasing the mission time of a SSC is more important for a SSC with a high failure to run probability.

  For example, turbine-driven pumps have a higher failure rate than motor-driven pumps, such as residual heat removal pumps. A sensitivity analysis can show whether a reduction (along with the necessary justification) would make a noticeable difference.
- Potential reduction in the mission time of a SSC normally secured early in the sequence as the result of the use of an alternate system that is modeled at the later part of the sequence.
- In the past, emergency diesel generator (EDG) mission time was reduced to account for the fact that recovery of offsite power during loss of offsite power (LOOP) and station blackout (SBO) sequences most likely occur well before the 24-hour PRA mission time. Therefore, to take credit for a lower failure-to-run (FTR) probability (which was historically high) due to lower run times, the 24-hour mission time for EDGs was replaced with the mean LOOP duration time of the composite of duration-weighted average of the four LOOP categories.

  The SPAR models now use the better method of convolution in the SBO model. Convolving the failure distributions eliminates the simplifying assumption that all failures happen at time zero.[13] The fundamental method used in the SPAR model for the inclusion of convoluted failure values include appending adjustment factors to specific cut sets. Adjustment factors in SPAR model are provided in time-dependent basic events (e.g., 30 minutes, 1 hour, 2 hours, etc.) for EDG FTR and nonrecovery of offsite power.
- Consult Idaho National Laboratory for adjustment of the convolution assumptions in the SPAR model.

4.4 Increasing Mission Time (Back to 24 Hours)

- Certain conditions involving failures, degradations, and unavailabilities may warrant increasing the mission time if already modeled less than 24 hours. Examples include:
  - A condition involving one system resulting in a longer mission time of an alternate system modeled as a part of the sequence.
  - A condition involving an increase in offsite power recovery time requiring extended EDG and turbine-driven auxiliary feedwater operations.
  - Increasing mission time due to implementation of alternative mitigation strategies (e.g., battery life extension).

[13] Quantification without convolution typically involves assumptions like: (1) FTR occurs very close in time to the demand for emergency power, (2) diesel repair begins immediately, and (3) time to core uncovery is constant over the mission time. Realistic quantification requires accounting for (1) the expected diesel failure time (1/λ) is well into the 24-hour mission time, (2) repair of the first diesel may be complete before the second diesel fails, and (3) the core uncovery time increases with each hour of successful diesel operation.

4.5 Increasing Mission Time (> 24 Hours)

For long duration LOOP events caused by an external event, the mission time of the EDG and other components may need to be increased to account for the fact that offsite power is not likely to be recovered (condition analysis) or was not recovered (initiating event analysis) within the 24-hour mission time.

4.6 Which Mission Time to Use– SPAR or PRA?

- ***Differences between the SPAR and Licensee PRA Models.*** When a comparison of results between the SPAR model and licensee's PRA identified a difference in a modeling assumption, then use the more realistic assumption after thorough evaluation of the supporting basis justified by rigorous engineering analysis or tests.

- ***Mission Time Coupling with Success Criteria.*** Typically, the mission time of a SSC is closely coupled with its success criteria and may be event and sequence dependent. The PRA mission time may not be applicable to the SPAR success criteria or assumptions used in Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) project post-processing rules. Check before applying a PRA mission time in the SPAR model.

- ***Considerations for Using a PRA Mission Time.*** Mission times used in the SPAR model are generic and may be conservative for select SSCs and sequences. Some considerations before using the licensee's PRA mission time in SPAR model:
  - Are the component/system success criteria similar to the SPAR model?
  - Does the SPAR model sequence and event thermal-hydraulic response change?
  - Does the SPAR model timing of operator actions change?
  - Do the emergency operating procedures support a shorter mission time (e.g., SSC secured early)?
  - Does the SPAR model event tree require modification?
  - Are the sequences and cut sets reasonable after applying PRA mission time?

4.7 SPAR Models– Modifying Mission Times

- ***Know Where the Basic Event Is Used in the SPAR Model.*** A basic event modification can adversely affect other parts of the SPAR model. Refer to Step 4 in Appendix A for considerations on this topic.

- ***Consistency between Systems in a Sequence.*** Mission times should be consistent with frontline and support systems associated with a sequence (e.g., cut sets in a given sequence should have mission times consistent with the sequence timing).

- ***Consistency between SSCs in a Fault Tree.*** Mission times should be consistent with other similar SSCs in a system fault tree (e.g., similar run times of motor-driven pumps).

4.8 SAPHIRE Code– Modeling Mission Times

- ***Options.*** Three options are available to modify the mission times for FTR parameters in SAPHIRE. These options include: (1) making a global change in mission time of FTR template event, (2) modifying the mission time of individual FTR basic events, or (3) using post-processing rules to replace a FTR basic event in the base SPAR model with a new FTR basic event with a different mission time.[14] For a basic event where a generic template event is used for similar components in different systems, a change would be applied in all fault trees that use the template event. In most ECAs, the change may be applicable to only specific sequences or cut sets. Post-processing rules may be used to replace a basic event with the mission time change.

  – *Make global changes to the SPAR model.* To make a global change in the mission time of a FTR template event in SAPHIRE, select the applicable template FTR basic event. Enter the new value in the *Mission Time* field. When completed click on *Apply* to complete the mission time modification.

  – *Modify the basic event.* Most FTR basic events in the SPAR model utilize two template events (FTR early and FTR late) to calculate the FTR basic event failure probability. Typically, the FTR-early template event represents the first hour of operation (after a successful start) and FTR-late template event represents the remaining 23 hours of operation (assuming the 24-hour PRA mission time. If the mission time is being modified to a value greater than one hour, the analyst should create a new FTR-late template event. To do this, select the current FTR-late template event (e.g., ZT-MDP-FR-L), modify the *Name* (e.g., ZT-MDP-FR-L1), and enter the new value in the *Mission Time* field, check the *Save As New* box, and click *Ok*. Then select the applicable FTR basic event (e.g., HPI-MDP-FR-1A), use the drop down menu for the original template event (e.g., ZT-MDP-FR-L) and scroll to find the new template event (e.g., ZT-MDP-FR-L1), and click *Ok*.[15]

    For FTR events that do not use templates events in this manner (e.g., air compressor), select the applicable FTR basic event, ensure the *Template Event* box is unchecked and *Default Template* field is set to NOT ASSIGNED. Then uncheck the *Failure Model* box, enter in the new value in the *Mission Time* field, and click *Ok*.

  – *Modify cut sets using post-processing rules in SAPHIRE.* Post-processing rules may be developed to replace a basic event in cut sets with a modified basic event with the mission time change. Post-processing rules may be applied to a particular fault tree, all fault trees, a particular event tree sequence, or all event tree sequences. The SAPHIRE instructions for creating post-processing rules in the SPAR models can be found in the SAPHIRE training manuals.

  No matter which option for modifying mission time(s) is used, the SPAR model must be re-solved to update the base model.

  – Select all of the event trees, right click and select SOLVE. Check the *Copy Cut Sets to Nominal Case* box and select SOLVE.

[14] Modifying a template event may result in a global change throughout the SPAR model for that component; however, some of the FTR basic events do not use template events. In addition, template events are not consistently used throughout the models; therefore, modifying the template may not make a global change for all the necessary basic events.

[15] If the analyst plans to run uncertainty analyses, the analyst should also clear the *Correlation Class* field.

4.9 PRA Standard Supporting Requirements– Mission Times

The supporting requirements from the PRA Standard for specifying an appropriate mission time for the modeled accident sequences, support systems, and intersystem and intrasystem dependencies are provided below for reference. The associated supporting requirement index number is also provided.

- ***Minimum Mission Time***. For sequences in which stable plant conditions have been achieved, use a minimum mission time of 24 hours. (SC-A5)

- ***Mission Time < 24 Hours.*** Mission times for individual SSCs that function during the accident sequence may be less than 24 hours, as long as an appropriate set of SSCs and operator actions are modeled to support the full sequence mission time. (SC-A5)

  For example, if following a loss-of-coolant accident, low-pressure injection is available for 1 hour, after which recirculation is required, the mission time for LPI may be one hour and the mission time for recirculation may be 23 hours.

- ***Mission Time > 24 Hours.*** For sequences in which stable plant conditions would not be achieved by 24 hours using the modeled plant equipment and human actions, perform additional evaluation or modeling by using an appropriate technique (SC-A5). Examples of appropriate techniques from Supporting Requirement SC-A5 include:
  - Assigning an appropriate plant damage state for the sequence;
  - Extending the mission time, and adjusting the affected analyses, to the point at which conditions can be shown to reach acceptable values; or
  - Modeling additional system recovery or operator actions for the sequence, in accordance with requirements stated in the Systems Analysis and Human Reliability sections of the PRA Standard, to demonstrate that a successful outcome is achieved.

- ***Mission Times for Support Systems.*** When modeling a system, include appropriate interfaces with the support systems required for successful operation of the system for a required mission time (SY-B9). Examples include:
  - Actuation logic,
  - Support systems required for control of components,
  - Component motive power,
  - Cooling of components, and
  - Any other identified support function (e.g., heat tracing) necessary to meet the success criteria and associated systems.

- ***Mission Times of Intersystem and Intrasystem Dependencies.*** The systems analysis shall provide a reasonably complete treatment of intersystem and intrasystem dependencies. Model the ability of the available inventories of air, power, and cooling to support the mission time. (SY-B11)

This page intentionally left blank.

5.0 Common-Cause Failure Modeling

5.1 Objective and Scope

- ***Objective.*** This section provides guidance for the treatment of common-cause failure (CCF) dependencies among components in a common-cause component group (CCCG) given an observed failure, and/or unavailability due to test or maintenance of one or more components in the CCCG.[16] This section provides guidance for adjusting the baseline CCF basic event probability of the CCCG in the standardized plant analysis risk (SPAR) model to best reflect the failure(s) that were observed in the operational event. Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) automatically calculates the CCF basic event probability for most cases encountered in event and condition assessments (ECA). This section applies to initiating event and condition analyses in Significance Determination Process (SDP), Accident Sequence Precursor (ASP), or Management Directive (MD) 8.3, "NRC Incident Investigation Program," assessments.

- ***In Scope.*** Applications that are in the scope of this guide include:
  - Treatment of CCF dependencies among components in a CCCG given one or more of the following observed conditions in an operational event:
    - An observed failure of one or more components in a CCCG.
    - An observed failure of one component and observed degradation in one or more remaining components in the CCCG.
    - Unavailability due to test or maintenance of one or more components in the CCCG.
    - An observed degradation in one or more comments in a CCCG, but no observed failure.

- ***Not in Scope.*** Activities that are outside the scope of this guide include:
  - Treatment of CCFs across system boundaries (e.g., circuit breaker used in different systems, electrical relays). SPAR models do not model CCF of similar components among different systems.
  - Modification of a CCF model in the baseline SPAR model (i.e., fault tree). Modifications to the SPAR model should be performed by Idaho National Laboratory.
  - Update, creation, or modification of CCF parameters (e.g., alpha factors). Modifications to CCF parameters should be performed by analysts specializing in the CCF data collection and parameter estimation.
  - Crediting defenses against CCF in risk-informed decision-making.

[16] A CCCG is a group of usually similar components (in mission, manufacturer, maintenance, environment, etc.) that are considered to have a high potential for failure because of the same cause or causes.

5.2 Ground Rules

The following three ground rules provide guidance to assist analysts in a consistent approach to the treatment of CCF in ECAs.

- ***Ground Rule 1.*** The performance deficiency (PD) that resulted in a failure in the CCCG has the potential for CCF of other components in the same CCCG.

  The PD identified in an inspection report is assumed to manifest a shared cause of potential failure of other “like” components in a system. Examples of performance deficiencies that represent the shared cause within a CCCG include, but not limited to, poor maintenance practices, inadequate plant procedures, failure to follow plant procedures, failure to implement effective corrective action, and inadequate design control.

  Consideration of defenses or coupling factors against CCF based on the observed PD and failure should be applied outside of the risk analysis (see Ground Rule 3). Such considerations are outside the scope of the current SPAR models and probabilistic risk assessments (PRAs).

- ***Ground Rule 2.*** The potential for CCF given an observed PD that resulted in a failure in the CCCG is the conditional CCF probability.

  In ECA, observed failures and deficiencies are mapped to the PRA model, but successfully operated and undemanded components are treated probabilistically at their normal failure probabilities. Analysis of operating experience data is used to estimate alpha factors for a CCCG. The Alpha Factor Model is used to estimate the conditional CCF probability in SPAR models. This conditional probability is the nominal (or baseline) probability of a CCF given an observed deficiency that resulted in a single failure in the CCCG. An observation of a single failure and not a CCF is considered a “success” in ECA with an alpha factor.

  This ground rule governs the arguments of successful tests, mission time window, and impossible failure mechanisms. These arguments are examples that are used to essentially credit observed “success” of other components in the CCCG. A successful operability test of redundant components in the CCCG in which the failure was observed does not reduce the conditional CCF probability of the remaining components to zero. Testing, inspection, or successful operations of the remaining components are needed to ensure the functionality of the remaining components to exclude partial or complete CCF, as well as good corrective action. However, these results do not change the conditional CCF probability given an observed deficiency that resulted in a failure.

- ***Ground Rule 3.*** Crediting observed defenses against CCF (i.e., successes) may be considered qualitatively outside the risk analysis.

  Specific programmatic licensee actions to defend against CCF coupling factors can reduce the occurrence of CCFs. However, in practice this is difficult to assess quantitatively in an ECA using the data-driven alpha factors. Therefore, it is recommended that, if appropriate, plant-specific defenses against CCF may be qualitatively considered in the SDP process by the Significance and Enforcement Review Panel (SERP). Such consideration may be appropriate if the analyst concludes that CCF is an influential factor in the risk assessment and a specific, programmatic licensee action to defend against CCF was in place to prevent or reduce the likelihood of an unforeseen PD impacting the remaining components in the CCCG. In such cases, the SERP will be risk informing the ECA results by giving credit for the successful CCF prevention action outside the risk analysis. A failure probability in the model or risk analysis result should not be "adjusted" to reflect the successful CCF prevention action.

An installed modification affected by a design control PD that degrades one component but was not implemented on the other components in the CCCG specifically to guard against CCF is one example of the potential application of this ground rule. In this case, the specific licensee action was to install and observe the modification in one component for some period of time before installing in another. The key to applying this ground rule is that the defense is deliberate and specific to prevent CCFs. When applying this ground rule, keep in mind that staggered installations may not rule out failures in the longer term.

5.3 Treatment of CCF in ECA– General

- ***Evaluate the PD.*** Generally, a PD that resulted in a failure of one component has the potential to fail other components in the CCCG within the system's mission time (see Ground Rule 1). Consider the PD in the broader context of CCF dependency and not in the context of the observed piece-part failure or failure mechanism. If a PD has yet to be defined in a MD 8.3 assessment, then assume that a PD exists.

  Inspection efforts will generally describe the PD and focus on the impact at the sub-component or piece-part level in detail. However, to identify CCF dependency, the analyst should focus on the PD in a broader context. Since the PD is normally defined as the proximate cause of the observed degradation, its impact on CCF should be defined at that level: "did not follow procedures", "did not evaluate and correct a degraded condition", and "did not conduct a functionality review". Human dependencies manifest into CCF at the organizational level—a level higher than the failed piece-part or failure mechanism.

  The inspection report may provide information that the other components in the CCCG were not degraded. For example, if the observed failed component in the CCCG experienced material degradation such as cracking due to inadequate corrective action, the report may discuss in detail the lack of observed cracking on the other components in the CCCG that were not failed. However, the analyst should identify CCF dependency based on the observed PD (i.e., inadequate corrective action) and not based on the actual as-found condition of the components that did not fail (see Ground Rule 2). As such, differences in piece-parts, failure rates, age, and manufacturer/model among components in the CCCG do not preclude CCF events at the broader level of a PD.

- ***Map the PD into SPAR Model.*** The analyst should consider the following to properly assign the conditional CCF probability for the observed PD.
  - *Choosing a CCF treatment category.* Apply one of the eight commonly used treatment categories, as appropriate. The categories are discussed in Table 5-1 (provided at the end of this section). For most performance deficiencies involving one component failure, the appropriate basic event of the failed component is set to TRUE and SAPHIRE will apply the appropriate conditional CCF probability based on the CCCG size. Consideration of special cases may include modeling the observed failure or extreme environmental condition resulting in a failure outside of the baseline CCCG model. Details of these treatment cases are provided in the table.

- – *Modifying the CCCG model.* Assignment of components to CCCGs is a qualitative analysis of similarity among components such that they would share a potential to fail from the same cause. If significant differences in design, maintenance, and operation are found to exist among components of a CCCG, and the analyst no longer believes the components are sufficiently similar, then it may be necessary to modify the CCCG model in the baseline SPAR model. This is expected to be rare given that various organizational problems can couple the components within a CCCG despite design differences at the piece-part or subcomponent level.

  If the failed subcomponent is unique to that failed super component, then consult Idaho National Laboratory to determine whether the subcomponent should be modeled explicitly in the fault tree. Note that the modification to the baseline SPAR model should be applicable for all applications, not just the ECA under consideration. If not, then the partitioning may be too narrowly focused on the piece-part or failure mechanism, and not on organizational factors that contribute to CCF dependencies. A review of the licensee’s PRA model may provide additional insights to CCF modeling of the failed component.

- – *Modeling explicit dependencies.* If the loss of function of a component is caused by the failure of another component outside the CCCG, then the analyst can either modify the CCCG model to explicitly include the failed component in the SPAR model with appropriate CCF modeling or the analyst can map the failure into the existing CCCG. This situation can occur, for example, if the actual failure occurs in a support system or a component that is not explicitly modeled in the SPAR model, or if a pre-initiator human error fails one or more components in the CCCG. In either approach, the analyst should consider the potential for dependent failures across the modeled components.

- – *Changing the failure probability of one or more components in a CCCG.* If the calculated failure probability of one or more components in a CCCG is modified by the analyst, SAPHIRE will calculate the related CCF basic event failure probability using the highest failure probability of the components in the CCCG.

- – *Modifying the SPAR model.* Modify the SPAR model to correct inaccuracies in the CCCG boundary or to explicitly account for dependencies, if necessary. Request support from the Idaho National Laboratory to modify the baseline SPAR model and CCF parameters. Idaho National Laboratory will review data for CCF events (e.g., n2, n3) and single events (i.e., n1) and generate modified or updated alpha factor parameters in accordance with established methods (e.g., NUREG/CR-6268, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding,” NUREG/CR-6823, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” and the PRA Standard). If no component-specific data is available, the use of the generic alpha factors will be considered. Modification to the SPAR model fault trees should be considered instead of data partitioning of alpha factor parameters.

- ***Calculate conditional CCF probability using SAPHIRE.*** In most cases, SAPHIRE will automatically calculate the conditional CCF probability for the CCCG. In cases where the component affected has start and run failure modes, the SAPHIRE SDP and ECA Modules will also automatically calculate the values for the unobserved failure modes. However, if the analyst is using the General Analysis Module or change sets in SAPHIRE, manual adjustments may be necessary.

5.4 Treatment of CCF in ECA– Other Considerations

- ***Apply Recovery, if Applicable.*** Consideration of recovery should be performed in accordance with the guidance in Section 6. Listed are a few items to specifically address when CCF is a significant contributor to the analysis results.
  - *Crediting recovery of the observed single failure.* For sequence cut-sets that involve an observed single failure, assess the potential for recovery of the failure using in Section 6.
  - *Crediting recovery of the cut-sets involving the CCF basic event.* For sequence cut sets that involve the CCF basic event that was impacted by the observed single failure, the potential for recovery should consider only the failure mechanism of the observed failure (if known). The other components in the CCCG could fail due to other mechanisms and may not be recoverable.

    For example, consider emergency diesel generator (EDG) A fails-to-start (FTS) in a two train CCCG and the observed failure was judged to be recoverable in the context of the applicable sequence. The minimal cut sets for EDG-A-FTS set to TRUE with a nonrecovery event applied are

    (EDG-B-FTR * EDG-A-FTS-NR)
    (EDG-B-FTS * EDG-A-FTS-NR)
    (EDG-CF-FTS * EDG-A-FTS-NR)
    (EDG-CF-FTR)

    The nonrecovery probability for EDG A will be based on the observed failure mechanism and piece-part failure (consistent with the failure memory approach).

    Note that the nonrecovery event should include other failure opportunities to restart and run. The treatment of recovery in the system fault tree is provided in Section 6.

- ***CCF implications of shared systems between plant units.*** The SPAR model typically includes a CCF basic event for components in a CCCG of shared systems between plant units, such as swing EDG or swing motor-driven auxiliary feedwater pump, in addition to a CCF basic event for components that are provided in the subject plant. The failure of a component in one plant may have a greater effect on risk at the other unit. Refer to Section 7 for modeling multi-unit considerations.

- ***Modification of CCF model and updates to alpha factor parameters.*** Update, creation, or modification of the baseline SPAR model (i.e., fault tree) or CCF parameters (e.g., alpha factors) should be performed by Idaho National Laboratory.

- ***Staggered test scheme assumed in SPAR models.*** SPAR models assume a staggered testing scheme for scheduled surveillance tests of components in a CCCG. SAPHIRE provide capabilities for calculating CCF probability based on either the staggered testing scheme (SPAR model default) or the non-staggered testing scheme, which can be selected by choosing *PLUGCCFAlpha* from the Failure Model Library on the Edit Basic Event menu.
  - Refer to the SAPHIRE User Guide (NUREG/CR-7039) for additional information on CCF compound events.

- ***CCF modeling in PRA is not cause-based.*** Therefore, selectively choosing CCF events from alpha factor estimates to revise the parameter or applying other ad-hoc adjustment factors to apportion alpha factors at a causal level is not appropriate.

5.5 CCF Treatment Cases

Categories of events that are expected to span the spectrum of cases encountered in ECA are provided below. Guidance is given for CCF treatment in each of these cases using the ECA Module in SAPHIRE. SAPHIRE calculates conditional CCF probabilities for each category.

- ***Treatment cases.*** Eight cases for treating an observed failure, degradation, or unavailability are summarized below.
  - Case 1– Observed failure with loss of function of one component in the CCCG.
  - Case 2– Observed failures with loss of function of two or more components in the CCCG.
  - Case 3– Observed failure with loss of function of one component in the CCCG—component not in SPAR model.
  - Case 4– Observed degradation in one or more components in CCCG without observed failure.
  - Case 5– Observed unavailability of a component in CCCG due to testing or planned maintenance.
  - Case 6– Observed loss of function of components in CCCG caused by the state of other components not in the CCCG.
  - Case 7– Observed loss of function of one or more components in CCCG as a result of environmental stress caused by failure or degradation of other components outside affected CCCG.
  - Case 8– No observed failure or degradation in the affected CCCG.
- ***Treatment methods.*** Six general methods for modeling a treatment case in SAPHIRE are summarized below.
  - P(CCF) = 1.0
  - P(CCF) = Conditional CCF probability (e.g., α_2 for CCCG=2, α_3 for CCCG=3) to account for the observed failure.
  - P(CCF) = Adjusted baseline CCF probability (i.e., $Q_{T(Degradation)}*\alpha_x$) for increased likelihood of single failure due to observed degradation.
  - P(CCF) = Adjusted baseline CCF probability for a reduced redundancy due to test or maintenance unavailability of a component.
  - P(CCF) = Baseline CCF probability (i.e., $Q_{T(Baseline)}*\alpha_x$) to account for no PD associated the CCCG.
  - Model inter- or intra-system interaction outside the CCCG model.
- ***Treatment guidance.*** Suggested guidance for applying the appropriate method of each case is provided in Table 5-1.

Table 5-1. Modeling approaches for typical treatment cases in ECA.

Category	Method
1. Observed failure with loss of function of one component in the CCCG and	• Apply P(CCF) = Conditional CCF probability (e.g., α_2 for CCCG=2, α_3 for CCCG=3) to account for the observed failure. – In SAPHIRE, set the failed component failure mode basic event to TRUE and SAPHIRE will apply the appropriate conditional CCF probability based on the CCCG size. – Basis: No credit for observed success. Given that the PD could have impacted the other components, but did not due to chance, is considered a success.
a. No other observed failures or degradations in other components in the CCCG were identified by inspections	
b. Other components in the CCCG were tested to be functional	
2. Observed failures with loss of function of two or more components in CCCG	• Apply P(CCF) = Conditional CCF probability (e.g., α_2 for CCCG=2, α_3 for CCCG=3) to account for the observed failures. – In SAPHIRE, set the failed component(s) failure mode basic event to TRUE and SAPHIRE will apply the appropriate conditional CCF probability based on the CCCG size.
3. Observed failure with loss of function of one component in the CCCG and component not in SPAR model	• Apply P(CCF) = Conditional CCF probability (e.g., α_2 for CCCG=2, α_3 for CCCG=3) to account for the observed failures. – In the SPAR model either change the model to explicitly model the component and its' CCCG or map the failure to an existing CCCG. Set either the newly added basic event or the existing basic event representing the failed component to TRUE and SAPHIRE will apply the appropriate conditional CCF probability based on the CCCG size. – Alpha factors will need to be estimated. Use alpha factors for similar components or the alpha factor prior distribution. Request assistance from the Idaho National Laboratory for modifying CCF parameters.
4. Observed degradation of one or more component(s) in the CCCG, but no loss of component function of any component	• No adjustment to P(CCF) is necessary because the conditional CCF probability already accounts for partial CCF events (degradations with no failures) in the alpha factor model. • Determine the failure probability of degraded component(s) to complete its 24-hour PRA mission time to reflect the increased likelihood of failure due to observed degradation. – Refer to Section 3 for guidance on failure determination and modeling. – Choose the approximate failure mode that the degradation would cause. – In SAPHIRE, enter failure probability of that component's single failure basic event failure mode. • If the component failure probability is increased, then apply P(CCF) = Adjusted Baseline CCF probability (i.e., $Q_{T(degradation)}*\alpha_x$) to account for increased likelihood of single failure due to observed degradation. – SAPHIRE will automatically adjust the baseline CCF probability by using the highest component failure probability (Q) in the CCCG in the (adjusted) baseline CCF calculation. • If the component failure probability is not adjusted, then apply P(CCF) = Baseline CCF probability (i.e., $Q_{T(Baseline)}*\alpha_x$). – In SAPHIRE, the baseline CCF probability is the default, if a basic event is not adjusted.
5. Observed unavailability of a component in the CCCG due to testing or planned maintenance	• Apply P(CCF) = Adjusted Baseline CCF probability for a reduced redundancy due to test or maintenance unavailability of a component. – In SAPHIRE set the test and maintenance basic event to TRUE.

Category	Method
6. Observed loss of function of Component B due to state-of-other System/Component A; no PD was identified with component B; and component A is outside component B's CCCG (CCCG_B):	*Examples include: inter-system interactions, such as, support system or I&C input losses; and intra-system interactions, such as flow diversion or strainer plugging.* • Determine whether the SPAR model's CCF alpha factor model for CCCG_B excludes or includes the state-of-other System/Component A. – Verify whether the observed inter- or intra-system interaction is modeled elsewhere in the SPAR model. – Verify whether CCF records associated with the inter- or intra-system interaction are used to calculate alpha factors for CCCG_B.
a. CCF model for CCCG_B excludes the state-of-other System/Component A	• Two modeling options: – Enhance the SPAR model to include component B dependence on System/Component A. This option is the preferred approach. – Use Component B and CCF model for CCCG_B as a surrogate for the system interaction. • For Option 1 (recommended), request assistance from Idaho National Laboratory to modify the SPAR model to include the system interaction. – Include an appropriate CCF model to account for CCF dependencies associated with the observed failure of Component A in System A (i.e., CCCG_A) that interfaces with or supports components in CCCG_B. – Follow quality assurance guidance when making changes to the SPAR model. Refer to Volume 3 of this handbook. – Apply P(CCF) = Baseline CCF probability (i.e., $Q_{T(Baseline)}*\alpha_x$) associated with CCCG_B to account for no PD identified with Component B. ○ In SAPHIRE, the baseline CCF probability is the default, if a basic event for Component B is not adjusted. – Apply P(CCF) = Conditional CCF probability (e.g., α_2 for CCCG=2, α_3 for CCCG=3) associated with CCCG_A, if applicable, to account for the observed failure of Component A. ○ In SAPHIRE, set the failed component failure mode basic event to TRUE and SAPHIRE will apply the appropriate conditional CCF probability based on the CCCG size. • For Option 2, carefully map the failure of system A into the fault tree model for Component B: – If component A does not fit into a CCCG of its own (e.g., CCCG = 1), then don't use this option—model Component A separately (see Option 1). – Verify that CCF model parameters (alpha factors) and CCCG sizes (CCCG_A, CCCG_B) are appropriate; otherwise, re-estimate parameters based on guidance in NUREG/CR-6268. – Verify that modifications do not adversely affect parameters used elsewhere in the SPAR model. Refer to the SPAR model, SAPHIRE manuals, and Volume 1 and Volume 3 of this handbook. Request assistance from Idaho National Laboratory. – If any parameter is adjusted for a conditional analysis, a recalculation of the baseline SPAR model may be required to reflect a higher risk profile of the surrogate model. No recalculation is necessary for initiating event analysis. – Follow quality assurance guidance when making changes to the SPAR model. Refer to Volume 3 of this handbook.

Category	Method
b. CCF model for $CCCG_B$ includes the state-of-other System/Component A	• Two modeling options: – Use the existing CCF model and parameters for $CCCG_B$. – Model the system interaction outside $CCCG_B$ and re-estimate parameters CCF model for $CCCG_B$. • For Option 1, the system interaction is implicitly modeled by the CCF model for $CCCG_B$. Although, an explicit model (Option 2) is preferable, Option 1 may give similar results without extensive resources for parameter re-estimates and SPAR model changes. – Request assistance from Idaho National Laboratory to evaluate the use of this option in this analysis application. – Verify that CCCG sizes ($CCCG_A$, $CCCG_B$) are appropriate; otherwise, explicitly model the interaction outside $CCCG_B$. – Apply P(CCF) = Conditional CCF probability (e.g., α_2 for CCCG=2, α_3 for CCCG=3) to account for the observed failure of component A and resulting unavailability of component B. ○ In SAPHIRE, set the failed component failure mode basic event to TRUE and SAPHIRE will apply the appropriate conditional CCF probability based on the CCCG size. • For Option 2, request assistance from Idaho National Laboratory to model the system interaction outside $CCCG_B$ and re-estimate parameters CCF model for $CCCG_B$. – Refer to the two options in the Case 5a.
7. Observed loss of function of Component B in $CCCG_B$ due to environmental stress caused by a failure or degradation of other components outside of affected CCCG:	Note: These cases present a failure or degradation of a component outside of System B that triggers an environmental stress-related failure of a component in $CCCG_B$. In addition, these cases may present one PD in either system or two different PDs, one in each system.
a. Failed component in $CCCG_B$ conforms to environmental qualifications (i.e., no PD associated with the components in the CCCG)	• Same as the inter-system interaction cases, above.
b. Failed component in $CCCG_B$ does NOT conform to environmental qualifications	• Apply P(CCF) = Conditional CCF probability (e.g., α_2 for CCCG=2, α_3 for CCCG=3) to account for the observed failure of component B and related PD. – In SAPHIRE, set the failed component failure mode basic event to TRUE and SAPHIRE will apply the appropriate conditional CCF probability based on the CCCG size.
8. No observed failure or degradation in the CCCG	• Apply P(CCF) = Baseline CCF probability (i.e., $Q_{T(Baseline)}*\alpha_x$). – In SAPHIRE, the baseline CCF probability is the default, if a basic event for component is not adjusted.

This page intentionally left blank.

6.0 Modeling Recovery and Repair

6.1 Objective and Scope

This section provides guidance for the treatment of recovery and repair actions of a failed or degraded structure, system, or component (SSC) that was observed in the operational event. The guidance addresses what recovery and repair actions can be credited in event and condition assessments (ECAs), and the requirements that should be met before crediting such actions. Definitions for recovery and repair action are provided. Also, guidance and considerations are provided for conducting recovery analyses and for modeling recovery/repair actions in the SPAR model. This section applies to initiating event and condition analyses in Significance Determination Process (SDP), Accident Sequence Precursor (ASP), or Management Directive (MD) 8.3, “NRC Incident Investigation Program,” assessments.

Guidance in this section is intended for modeling recovery and repair actions in ECA. Although this guidance can be used to model recovery actions in the base case model, other guidance related to building probabilistic risk assessment (PRA) models should be reviewed for completeness.

6.2 Background

- ***Definitions: Recovery and Repair.*** In PRA, there is a clear distinction between actions to repair components or systems and actions to recover components or systems. The following definitions are from NUREG/CR-6823, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” and the PRA Standard.[17]
  - Recovery actions involve the use of alternate equipment or means to perform a function when primary equipment fails, or the use of alternate means to utilize equipment that has not responded as required. The PRA Standard defines as “*. . . restoration of a function lost as a result of a failed structure, system, or component (SSC) by overcoming or compensating for its failure.”*

    Examples of recovery actions include opening doors to promote room cooling when an heating, ventilation, and air conditioning system fails, recovering grid-related losses of offsite power by rerouting power or using alternate mitigating strategies (e.g., FLEX equipment), manually initiating a system when the automatic actuation signal fails, bypassing trip logic using jumper cables, and using a hand wheel to manually open a motor-operated valve when the motor fails to operate.
  - Repair actions involve the actual repair of the mechanism, which caused a component or system to fail. The PRA Standard defines repair as *“. . . restoration of a failed SSC by correcting the cause of failure and returning the failed SSC to its modeled functionality.*”

    Examples of repair actions include repairing weather-related losses of offsite power, repair of a pump that failed to start, or replacement of a failed circuit breaker.
- ***Overview: Modeling recovery and repair actions in PRAs.*** PRA models typically include

[17] The PRA Standard referred in this handbook includes ASME RA-Sa-2009, as endorsed by Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities.”

a number of *recovery actions* of the type identified in the examples above. However, because recovery actions can involve complicated actions that are governed by procedures, most are typically evaluated using human reliability analysis (HRA) methods. A general exception is the treatment of offsite power recovery where the required recovery actions are often not within the jurisdiction of the plant personnel. Thus, offsite power recovery data is collected and reduced for use in PRAs. Recovery of an emergency diesel generator is another action commonly modeled in PRAs based on actual data. The repair of components is generally not modeled in base PRA models because one or more of the following apply to most cut sets and sequences: (1) the time available to repair most components is generally too limited (i.e., core damage would occur before the repair is completed), (2) repair is an action that is not always governed by procedures and thus difficult to justify, (3) the availability of spare parts cannot always be certain, and (4) abnormal procedures generally direct operators to use alternative equipment as a first priority. HRA techniques for estimating likelihood of successful repair should not be used because the possible repair scenarios that are affected by a variety of human actions and hardware-related issues that would not be known without knowing the specific causes of the problem.

  – *There are exceptions to these general observations.* For example, the replacement of fuses is an action identified in some fire abnormal procedures and can be accomplished rather quickly since spare fuses are available. As with a recovery action, either an HRA or data reduction approach could be utilized to generate a failure probability for a repair action. The modeling of recovery and repair actions in PRA reflects the need to accomplish the action within some time frame (e.g., before core damage occurs). Thus, the collected data must include both the time of failure and recovery to be utilized in the PRA.

- ***Overview: Modeling Recovery and Repair Actions in ECA.*** The modeling of repair actions is limited in PRAs for the reasons stated above. The modeling of recovery actions in the PRA may be incomplete due to a new or recently proven alternate mitigating strategy. In an ECA where a failed SSC is the focus of the assessment, crediting a recovery or repair action may significantly reduce the risk significance of the unavailability. In addition, specifics are known about the ability to recover a specific failure that may lend itself to modeling, whereas the estimation of a generic recovery event in the base case PRA may not be practical. The consideration and process for recovery/repair modeling in event assessment generally follows the same guidance for building PRAs.

6.3 Treatment of Recovery/Repair Actions in ECA– General[18]

- ***PRA Standard requirements.*** Actions to recover/repair an observed failure of a SSC can be considered and modeled in accordance with supporting requirements of the PRA Standard. For the most part, these supporting requirements can be used to model recovery and repair actions in an event assessment.

  – The supporting requirements from the PRA Standard for crediting and modeling

[18] The terms “recovery”, “repair”, “recovery event”, and “nonrecovery” are often used interchangeably in risk analyses of operational events. In this handbook, the definitions from the PRA Standard are used to define recovery actions and repair actions. No standard definitions exist for the other two terms. Therefore, for the purpose of this handbook, a recovery event means human actions to restore a failed SSC or lost function, including the repair action, if any. “Nonrecovery” probability means the failure probability of the recovery event. In some cases, other actions needed to restore a lost function may be modeled separately in the event tree; therefore, a recovery action may not restore a lost function in itself.

recovery and repair actions, including associated index numbers, are provided in Section 6.6.

  - An overview of applicable supporting requirements in Section 6.6 include the following considerations:
    - ○ Demonstration that the action is plausible and feasible for the scenarios to which recovery/repair action are applied (HLR-HR-H).
    - ○ Availability of procedures, operator training, cues, and manpower (HR-H2).
    - ○ Relevant scenario-specific performance shaping factors in the HRA (HR-H2 and HR-G3).
    - ○ Dependencies between human failure events (recovery, repair, and emergency operating procedure actions) in the sequence, scenario, or cut set (HR-H3, HR-G7, and QU-C2).
  - Additional supporting requirements apply to the modeling of data-based “nominal” repair failure probabilities in the base case PRA. NUREG/CR-6823 provides guidance for allocating repair and recovery data.

- ***Using Data to Estimate Nonrecovery Probabilities.*** Nominal failure probability for a *repair* action is normally based on the evaluation of industry-wide operating experience data. Examples of data-based nonrecovery probabilities used in SPAR models include recovery/repair of emergency diesel generator (EDG) failures and loss of offsite power (LOOP) events.
  - Guidance on the process for collecting and reducing recovery and repair data is provided in Section 5.3 of NUREG/CR-6823. This guidance includes a description of the type of data that is reviewed and guidelines for allocating data.
  - A decision or procedural direction to perform deep direct-current (DC) load shed early in some events [e.g., station blackout (SBO)] may complicate recovery of AC power or EDGs, and this condition should be taken into consideration by the analyst when estimating nonrecovery probabilities.
  - Analysts specializing in parameter data collection, reduction, and statistical analysis should be consulted for estimating a nonrecovery probability using operational experience data.

- ***Using HRA to Estimate Nonrecovery Probabilities***. Failure probability for a recovery action is normally derived in a HRA. Good practices from NUREG-1792, “Good Practices for Implementing Human Reliability Analysis,” for crediting post-initiator recovery actions while implementing Regulatory Guide 1.200 and the related requirements of the PRA Standard are summarized below.
  - *Good Practice #1: Define Appropriate Recovery Actions.* Based on the failed functions, systems, or components, identify recovery actions to be credited that are not already included in the PRA (e.g., aligning another backup system not already accounted) and that are appropriate to be implemented by the crew to restore the failure. Aspects to consider are included in the questions listed in Section 6.7.
  - *Good Practice #2: Account for Dependencies.* The good practices provided for post-initiator human failure events (HFEs) in general apply specifically to recovery

actions as well.[19] Particular attention should be paid to accounting for dependencies among the HFEs including the credited recovery actions. Considerations for accounting for dependencies are provided in Section 6.4 and Section 6.8.

- Good Practice #3*: Quantify the Probability of Failing to Perform the Recovery.* Quantify the probability of failing to perform the recovery by (1) using representative data that exists and deemed appropriate for the recovery event, or (2) using the HRA method/tool(s) used for the other HFEs (i.e., using an analytical/modeling approach).
- If using data, ensure the data are applicable for the plant/sequence context or that the data are modified accordingly.
- In addressing the above issues and assessing which recovery action, or actions, to credit in the PRA, for post-initiator HFEs all the good practices provided in the following sections in NUREG-1792 apply (i.e., the failure to recover is merely another HFE, like all of the other post-initiator HFEs):
  - Section 5.1, "Identifying Potential Post-Initiator HFEs"
  - Section 5.2, "Modeling Specific HFEs Corresponding to Human Actions"
  - Section 5.3, "Quantifying the Corresponding Human Error Probabilities (HEPs) for Post-Initiator HFEs"

6.4 Treatment of Recovery/Repair Actions in ECA– Other Considerations

- ***Considerations for Determining Recovery/Repair Actions are Plausible and Feasible.*** A thorough recovery analysis requires careful consideration (at the cut set or scenario level) of the appropriate performance shaping factors in the HRA. Some questions to consider for crediting and modeling the recovery/repair of an observed failure are provided in Section 6.6. These questions were developed largely from the PRA Standard, NUREG-1792, and experience from SDP and ASP analyses.

- ***Exceptions to Requirements and Considerations.*** In general, no recovery or repair action should be credited where any of the considerations in Section 6.8 are not met (e.g., there is not sufficient time, there are no cues that there is a problem, there are not sufficient resources, and there is no procedure or training).
  - It may be possible to justify exceptions in unique situations, such as a procedure is not needed because the recovery/repair is a skill-of-the-craft, non-complex, and easily performed; or the specific failure mode of the equipment is known for the sequence (this is usually not the case at the typical level of detail in a PRA) and so repair of the failure can be credited because it can be easily and quickly diagnosed and implemented.
  - Any exceptions should be documented as to the appropriateness of the recovery/repair action.

- ***Consideration of Observed Errors, Failures, and Successes.*** Once an observed failure was judged recoverable or repairable given cut set-specific time constraints, the failure probability for a recovery or repair action can be estimated based on cut set-specific HRA and observations from the actual repair of the component.
  - Difficulties, error, and failures that were observed during the recovery/repair should be

[19] A HFE is defined as a basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or inappropriate action.

considered in the HRA (and in the recovery/repair plausibility and feasibility determination). This is consistent with the "Failure Memory Approach."[20]

  - Similarly, recovery/repair actions that were performed successfully during the event should be addressed in cut set-specific HRAs, given that successes are treated probabilistically in the "Failure Memory Approach."

- ***Consideration of Operator Intervention Preventing a Catastrophic Failure.*** For most cases, the observed end state of the SSC failure is given as the figure of merit. The recovery analysis is usually based on this observed end state. However, a catastrophic failure should be postulated probabilistically for those cases where human intervention prevented the failure to reaching a non-repairable end state. This consideration is consistent with the "Failure Memory Approach" for the treatment of success (e.g., successful avoidance of a catastrophic failure). These cases could apply to a degradation found during a surveillance test or unplanned demand where the operator secured the component before catastrophic failure. The probability that the operator intervention would not occur should be considered in the recovery analysis.

  For example, a recovery analysis would consider the probability that an auxiliary operator that is typically dispatched to an operating turbine-driven auxiliary (AFW) pump following a reactor trip (per administrative procedure) would not reach the pump room in time to prevent a catastrophic failure due to a repairable lubricating oil leak.

- ***Consideration of Support System Availabilities.*** Ensure that support systems are available in the sequences in which recovery/repair is applied. Availability of support systems may need to be verified multiple times during events [e.g., initially upon SBO and once extended loss of AC power (ELAP) has been declared] to account for changes in support system availability. Additional complications from loss of support systems (e.g., additional operator actions to maintain level to avoid filling steam lines with high level trips disabled and wider level bands) should be considered under the appropriate section of this manual (e.g., Section 9.0 for new HFEs).

- ***Examples of Failure Events and Associated Potential Recovery Actions.*** Table 6-1 below provides examples of failure events and associated potential recovery actions.

- ***Modeling Recovery of Test and Maintenance Unavailabilities.*** The recovery analysis should consider probabilistically the period of time that a SSC in a test or maintenance activity could not be restored to service given a postulated unplanned demand. This consideration is especially important for maintenance activities when the component is fully disassembled. For cases when the system is being tested during a routine surveillance activity, the restoration may be possible during the entire unavailability period.

- ***Modeling Multiple Recovery/Repair Actions.*** Considerations for crediting and modeling more than one recovery/repair actions (i.e., how many recoveries to be credited in one accident sequence/cut set) include the following:

  - Recovery/repair of failures in one system should be limited to one failed component in

[20] The "Failure Memory Approach" is used to estimate the risk significance of operational events. In the "Failure Memory Approach," basic events associated with observed failures and other off-normal situations are configured to be failed or degraded, while those associated with observed successes and unchallenged components are assumed capable of failing with nominal probability.

the system (i.e., recovery/repair limited to one train in a multiple train system).

For example, if two EDGs failed, then plant staff would most likely focus on the less problematic diesel for recovery. Therefore, the recovery credit would be assigned to the EDG that can be restored to service earlier. Failure to recover the less problematic diesel would most likely lead plant staff to focus on alternate mitigating strategies (e.g., FLEX, deployment of additional portable equipment). These actions should be evaluated as multiple recovery/repair actions as indicated below.

Table 6-1. Examples of failure events and associated potential recovery actions

Examples of Initial Failure Event(s)	Potential Recovery/Repair Action(s)
Automatic actuation fails.	Manual actuation.
Operator fails to recognize the need to take action (diagnosis failure).	Additional cues or re-visitation.
Test and maintenance unavailability.	Restore to service (if according to Technical Specifications the SSC is considered inoperable while in test/maintenance but can be returned to service quickly); or alternate mitigating strategies (e.g., FLEX, additional portable equipment).
Failure on demand (electrical, e.g. fuse or other electrical fault which can be recovered).	Replace fuse or if a control power problem, manually shut the local breaker.
Failure on demand (mechanical).	Use redundant SSC or a functionally similar component (e.g., opposite train/alternate mitigating strategies); or repair.
Failure to run.	Similar electrical / mechanical considerations as in failure on demand.
System level failure (e.g. loss of CCW system or loss of offsite power as an initiating event).	Empirical system recovery data; or alternate mitigating strategies (e.g., FLEX, additional portable equipment).

– Recovery/repair of failures in two systems may be a burden on plant staff, except when ample time and staffing exists to recover two failures or the recovery/repair of one failure is a simple reset action.

  For example, diagnosing and recovering simultaneous failures of the AFW and high-pressure injection systems may be difficult within the short time available, whereas, recovery of AFW and residual heat removal systems may be more likely. A quick recovery of one system involving trip reset from the control room may allow operators to diagnose and recover another system failure.

– Multiple recovery/repair actions in a cut set should be checked to determine whether such credit is reasonable based on available time and staffing.

  For example, consider that one recovery may be tried (perhaps even multiple times) and then the second recovery may be tried but with even less time and resources available because of the attempts on the first recovery. Hence, the failure probability of the second and any subsequent recovery actions should be based on more pessimistic characteristics (e.g., less time available, less resources) than if such a possibility is not considered. The possibility of single point failures impacting a recovery event should also be considered (e.g., having multiple FLEX high-pressure injection pumps available would not yield a credible recovery event given the failure of the suction hose, with no available spare, that is common to all pumps).

- ***Consideration of Alternate Mitigating Strategies*.** Plant licensees have implemented alternate mitigating strategies (e.g., B.5.b. measures, FLEX) in response to NRC orders. These strategies often involve the use of non-safety, portable, manual control, offsite, or non-standard system alignments. Crediting of these strategies in risk assessments should meet the guidelines outlined in Regulatory Information Summary 2008-15, “NRC Staff Position on Crediting Mitigating Strategies Implemented in Response to Security Orders in

Risk-Informed Licensing Actions and in the Significance Determination Process." Consideration for incorporation of manual actions, special equipment operation, or other non-standard actions into the risk assessment include, but are not limited to:

- Operators diagnosis of the ability and need to use the alternate strategy,
- Feasibility of alternate strategy in the scenarios of interest to include engineering analysis or system testing showing the strategy to be successful throughout the accident scenario,
- Deployment (if applicable) of the equipment,
- Support systems and instrumentation availability,
- Environmental conditions,
- Reliability of associated equipment considering frequency of maintenance and testing intervals,
- Time margin for successful implementation of strategy,
- Procedural direction in the scenarios of interest,
- Training provided for staff responsible for actions within the strategy,
- Staffing levels and availability of personnel for performing actions associated with the strategy, and
- Safety/security interface considerations.

Credit for alternate mitigating strategies must be included in both the baseline PRA model and the assessment of the non-conforming condition due to the performance deficiency, unless the action would only apply for the latter event. For example, if equipment is available that could reduce the risk; the analyst should consider whether the equipment could also be used for scenarios in the baseline model. Otherwise crediting the equipment in the SDP but not the base model would result in a smaller estimate of the risk increase than is realistic. For more information about where to model alternate mitigating strategies in the PRA, see Section 6.5.

Nuclear Energy Institute's (NEI) FLEX in Risk-Informed Decision Making (FRIDM) Task Force developed guidelines for the industry to follow when requesting credit for alternate mitigating strategies. This guidance is contained in two white papers, "Qualitative Assessment for Crediting Portable Equipment in Risk-Informed Decision Making," and "Streamlined Approach for Crediting Portable Equipment in Risk-Informed Decision Making." The NRC has not endorsed this guidance; however, a letter from the Office of Nuclear Reactor Regulation (NRR) Office Director was issued (ADAMS Accession No. ML16167A034), which captured NRC staff's views on the white papers. NEI subsequently submitted NEI 16-06, "Crediting Mitigating Strategies in Risk-Informed Decision Making," for information only to the NRC. This document has three sections, the first two representing the contents of the two white papers and a third section providing guidance to licensees about crediting portable equipment in a PRA. This section was reviewed by NRR staff and a publicly available memorandum (ADAMS Accession No. ML17031A269) was issued to capture the staff's comments. The above referenced documents should be considered information only to NRC risk analysts as background information on how licensees may credit alternate mitigating strategies in their risk assessments.

Ultimately, the decision to provide credit for alternate mitigating strategies that are not explicitly modeled in the subject plant's SPAR model is up to the analyst based on, but not limited to, the factors expanded on in this section.

- ***Consideration of Dependencies among Multiple Human Actions in a Cut Set***. Particular attention should be paid to accounting for dependencies among the HFEs including the credited recovery/repair actions. Considerations from NUREG-1792 include:
  - Dependencies should be assessed:
    - Among multiple recoveries in the accident sequence/cut set being evaluated
    - Between each recovery and the other HFEs in the sequence/cut set being evaluated
  - As part of this effort, the analyst should give proper consideration to the difficulties people often have in overcoming an initial mindset, despite new evidence.

    For example, consider how long the power-operated relief valve path remained open in the Three Mile Island accident, despite new cues of the problem, different personnel arriving, etc.
  - The determination of whether there is dependence between HFEs and the level of dependence (if there is dependence) needs to be adequately justified and documented to ensure that credit for the recovery action(s) is appropriate. Refer to Section 9.3 for further information on dependence.

- ***Extending Recovery/Repair Time (Failure to Run Events).*** A component failure, after the component had operated for some of its mission time (even 10 minutes or so), can help to extend the time to core uncovery. Reduced decay heat rate, full steam generators (pressurized-water reactors), or reactor vessel (for boiling-water reactors) extends the time before core uncovery, thus allows for more recovery/repair time.

  For example, at a 4-loop Westinghouse plant, failure of the turbine-driven AFW pump after 2 hours following a SBO can result in doubling the time to core uncovery.

  Some considerations when crediting recovery/repair from a fail-to-run (FTR) event:
  - *Increase in time available for diagnosis and operator actions.* Extended time may increase the Time Available performance shaping factor (PSF) of the recovery/repair actions.

    For example, failure of the last running AFW pump at 3 hours after reactor trip would increase the available time to initiate feed and bleed actions due to lower decay heat rate and full steam generator(s).
  - *Thermal-hydraulic basis of event tree function.* The basis for changing the success criteria of a system based on extended time to core damage from a FTR event should be compatible with the appropriate thermal-hydraulic response. The timing of sequences (core damage/uncover times) used in event trees are usually based on the assumption that failure-to-start (FTS) and FTR events occur at t = 0.
  - *Reduced mission time.* A recovery/repair of a component that fails to run will reduce the mission time that the component/system has to run, after recovery/repair, to complete its 24-hour mission. However, the successful operation of the component/system before the failure must be probabilistically modeled (consistent with the "Failure Memory Approach") in the PRA using nominal FTR probability during the first part of the mission time segment.

6.5 SPAR Model Modifications– Considerations

- ***Consult Idaho National Laboratory.*** Changes to the SPAR model should be closely coordinated with the Idaho National Laboratory staff to ensure changes are completely reflected throughout the model and changes are made in accordance with the SPAR model quality assurance program. Review checklists for SPAR model modifications are provided in Volume 3 of this handbook.

- ***Where to Add the Recovery Event: Event Tree, Fault Tree, Sequence, or Cut Set.*** Recovery/repair actions can be added at various levels in the SPAR model: event tree, fault tree, sequence, or cut set. The appropriate level depends on how narrow the application of the recovery/repair action is desired. All applications will require a basic event in a fault tree, either the use of an existing basic event or the creation of a new basic event. A post-processing rule can be developed or an existing rule edited to replace the recovery/repair basic event with time-dependent probabilities at the cut set, sequence, or event tree top event level.

  Considerations for adding a recovery event at the various levels in the SPAR model include:[21]

  – *Event tree level.* Examples when a recovery event is typically applied in the event tree top event include recovery from an initiating event (e.g., loss of instrument air, loss of service water, loss of offsite power) and recovery of another top event (e.g., loss of main feedwater, loss of primary conversion system). However, post-processing rules may be needed to apply a time-dependent recovery action (e.g., EDG nonrecovery probabilities) at the sequence or cut set level.

  – *Fault tree level.* Modeling recovery and repair actions are nominally included at the fault tree level. However, as with event tree applications, post-processing rules may be needed to apply a time-dependent recovery action at the sequence or cut set level. Further, a modified fault tree with configuration-specific structure and/or probabilities may be required for unique event-specific situations. In this case, the analyst may find it easier to copy and rename an existing fault tree, modify as desired, and apply the new fault tree in a sequence via a linking rule.[22]

    ○ Locate where the fault tree is used in the SPAR model. If the recovery/repair action only applies to a subset of sequences, then use linking rules to apply a modified copy of the fault tree with recovery/repair action to the sequences of interest.

  – *Sequence level.* Linking rules are typically applied at the sequence level to replace an original base case fault tree with a modified copy of the fault tree (with a different name) that includes the recovery/repair action. Refer to the above for additional considerations for applying recovery/repair actions to fault trees.

  – *Cut set level.* Applying recovery/repair actions at the cut set level is a common method for ensuring that the time-dependent nature of the recovery or repair action is properly modeled. Post-processing rules are used to replace or append an existing basic event in a cut set with another that includes the failure probability of the action. However, the

[21] In addition, see the considerations in “Using an existing recovery event in the SPAR model” in Section 6.4 when reusing existing basic events and post-processing rules.

[22] SAPHIRE Link Event Tree Rule (or linking rule) Editor creates a linking rule that replaces the original top event with a substituted top event based on the logical conditions dictated by the rule.

applicable cut sets must be identified before the post-processing rules can be written. Considerations include:

  - ○ To ensure that all important cut sets in which the recovery or repair action are identified, an initial scoping model solution should be performed with the failed event probability set to 1.0. Setting probability to 1.0, rather than a logical failure (i.e., TRUE), would ensure that the corresponding basic event appears in the minimal cut set list generated by the quantification process. However, the model solution will result in non-minimal cut sets.
  - ○ Look for dependencies between the recovery event(s) and other events in the cut sets.
  - ○ Write post-processing rule(s) to account for identified dependencies.
  - ○ In the final quantification (model solution), the failed event would now be set to TRUE, in order to ensure that a correct minimal cut set equation is generated.

- ***Where to Apply the Recovery Event: Base Case Model or Change Case.*** The analyst must decide whether to add the recovery or repair action in the base case SPAR model or the change case. Applying a recovery/repair basic event in the base case model may lower baseline core damage frequency (CDF), thus increasing the change in core damage frequency (ΔCDF) in select sequences. Applying the event in the change case and setting the event to FALSE in the base case model may increase baseline CDF, thus decreasing ΔCDF in select sequences. For most cases in ECA, applying a recovery or repair action to cut sets associated with the observed failure will not result in a difference in the results. Some considerations for modeling recovery and repair actions include the following:

  – *Applying recovery actions of pre-planned strategies.* Recovery actions should be modeled in the base case SPAR model. These actions are usually pre-planned using installed systems with pre-staged hardware, tools, procedures, and training. Given that the intended reason to include a recovery action in the PRA model is to take credit for risk reduction in the overall plant CDF, the recovery event should be applied to the base case PRA model.

    - ○ For a data-derived nonrecovery probability already included in the base case model, the basic event parameter inputs (i.e., random failure data, uncertainty data) in the base case model may be replaced with the parameters associated with the HRA-derived estimate.
    - ○ For a HRA-derived nonrecovery probability already included in the base case model, human errors that were observed during the recovery/repair should be considered in a failure-specific HRA to re-evaluate the nonrecovery probability. The basic event parameter inputs in the change case should include parameters associated with the HRA-derived estimate.

  – *Applying repair actions of observed failures.* Repair actions of observed failures can be modeled in the change case. These actions are usually ad hoc; therefore, the HEP will be failure-specific. Event-specific risk reduction is usually credited in the change case.

    - ○ If a data-derived nonrecovery probability is already included in the base case model (e.g., EDG repair), then either
      - ▪ Set the recovery event in the base case model to TRUE or FALSE (no difference) and replace the basic event parameters (i.e., random failure data, uncertainty data) with the HRA-derived estimate in the change case; or

        - Change the basic event parameter inputs with the HRA-derived estimate in the base case model and make no changes in the change case.

  - *Applying recovery actions associated with alternate mitigating strategies*. As a general rule, an alternate mitigating strategy, if it meets the appropriate criteria established in this section to be credited, should be modeled as a recovery action (as defined in the PRA Standard) in the base case model instead of a repair action in the change case, especially when the creditable action has been already modeled in the PRA.

- ***Using an Existing Recovery Event in the SPAR Model***. The base case SPAR model contains few recovery events that include basic events and post-processing rules with nominal failure to recover probabilities (e.g., EDG, LOOP). In addition, some SPAR models may include legacy events and rules that are not used (set to TRUE). Considerations for the use of an existing recovery event are summarized below and discussed further in the subsection.

  - Recovery/repair actions in SPAR models are noted by “XHE-XL” in the basic event name.
  - Know where the basic event (and fault tree) is used in the SPAR model.
  - Review post-processing rules used in the base case SPAR model for applicability.
  - Evaluate that the fault tree logic is correct for its intended modified use.

- ***Know Where the Basic Event or Fault Tree Is Used in the SPAR Model.*** Check that a proposed modification to an existing basic event or fault tree does not adversely impact the use of the same basic event or fault tree elsewhere in the SPAR model. The modification may not be appropriate in all sequences, especially for time-dependent recovery/repair actions.

  Some considerations include the following:

  - Examples where a modification of a basic event can affect multiple parts of the model include:
    - Basic event used in different fault trees,
    - Basic event used in a compound event [e.g., common-cause failure (CCF)],
    - Template event shared by basic events of a component group (e.g., motor-driven pump, motor-operated valve), and
    - Basic event used in post-processing rules.
  - Examples of basic event parameter variables that could impact multiple parts of the model include:
    - Failure probability/rate,
    - Mission time,
    - Calculation type, and
    - Process flag.
  - The same fault tree can be used in several event trees.
  - A new basic event or fault tree may be easier to apply in the SPAR model.

- ***Review SPAR Model Post-Processing Rules.*** Post-processing rules are free-form logic rules that allow for the alteration or deletion of fault tree or sequence cut sets in a "post-processing" fashion. Post-processing rules are used in SPAR models to apply recovery/repair events and other types of basic events in the appropriate cut sets after the change set is generated and the sequences are solved.
  - The post rules employed during the model solution should be reviewed to understand how the rules impacted dominant cut sets. Such rules may remove cut sets or significantly reduce the cut sets' probability. Confirm that any such rules are appropriate for the analysis and modify as necessary.
  - Post-processing rules may be developed for the following cases:
    - Particular fault tree (Fault Tree Rule Level)
    - All fault trees (Project Rule Level)
    - Particular sequence (Sequence Rule Level)
    - Single event tree (Event Tree Rule Level)
    - All sequences (Project Rule Level)
  - A list of each type of recovery rule can be viewed in Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE).

- ***Adding a Recovery Event in a Fault Tree.*** Considerations for adding a new recovery event in an existing fault tree include the following:
  - *Include nominal failure probabilities associated with restart.* When modeling the recovery/repair of an observed failure, include nominal probability of hardware failures during and after restart attempt. Components can FTS and FTR after they are successfully recovered or repaired. This is important for failure modes with high failure probabilities (e.g., a failure mode probability that is on the same or greater than the nonrecovery probability). Since the component event is set to TRUE, a sub-tree will be needed to model the recovery and operation of the component during restart and throughout the remainder of its mission time.
  - *Example of using the correct fault tree logic.* An example of sub-tree logic for a repair model that can be added to an existing fault tree is shown in Figure 6-1. Elements of the sub-tree example are summarized below.
    - A new recovery event [*Operator Fails to Repair Motor-Driven Pump (MDP) 3A*) is created and the failure probability is set to the HRA-derived estimate (HEP = 0.1) in the change case to represent observed failure and cut set dependences. If HEPs are cut set dependent, then post-processing rules are used to replace the "place holder" recovery event with the cut set-specific recovery events (not shown). Each of these recovery events will have a unique name and parameter values. This recovery event should be set to FALSE in the base case model.
    - The original FTS basic event (*MDP-3A Fails to Start*) is moved to the sub-tree and the failure probability is set to TRUE in the change case. This basic event must remain in the model, since it is used in the CCF compound event for that failure mode (not shown). Note that the logic does not allow the propagation of the TRUE value up the tree.
    - A new basic event (*MDP-3A Fails to Restart*) is created to model the probability of

failure to restart following repair. This failure probability (and other basic event parameter inputs) is normally set to the nominal value for that failure mode, i.e., same parameters used in the base case model basic event (MDP-3A Fails to Start). This recovery event should be set to FALSE in the base case model.

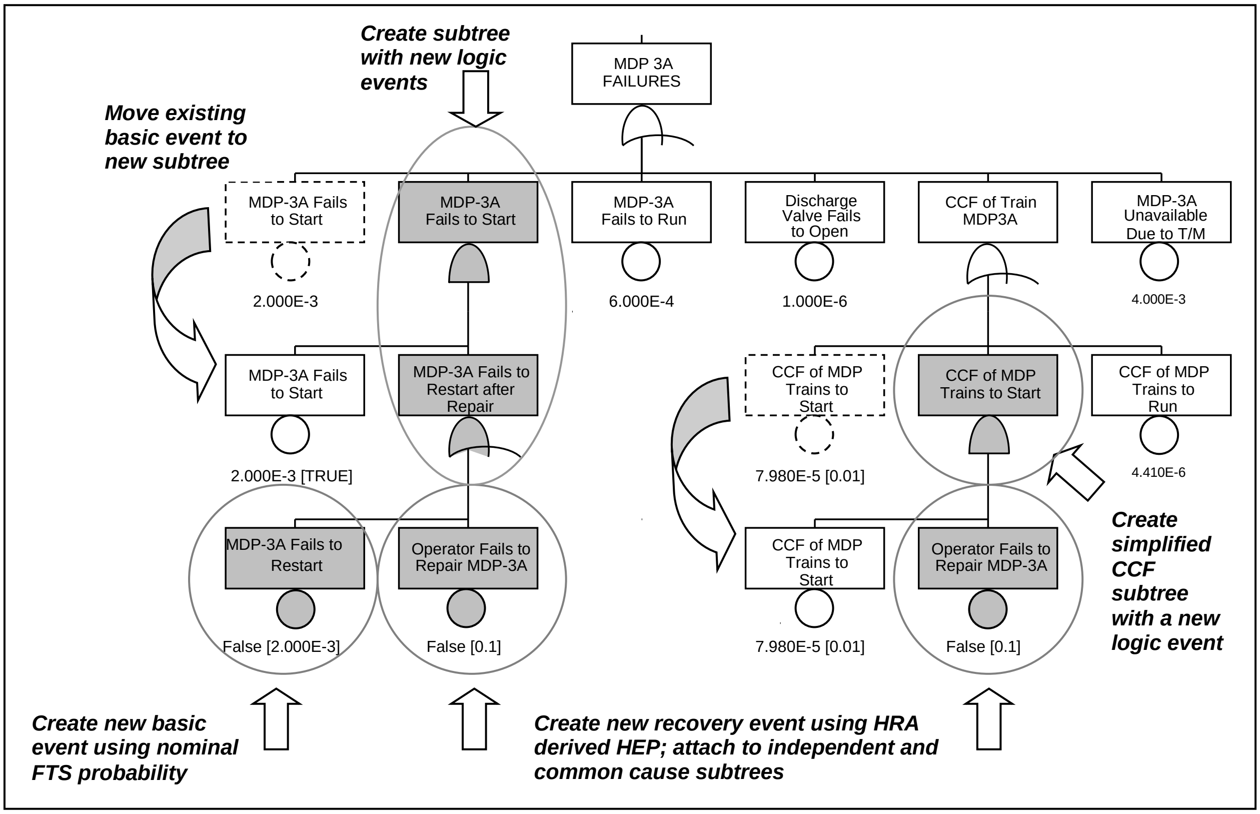

Create subtree with new logic events
MDP 3A FAILURES
Move existing basic event to new subtree
MDP-3A Fails to Start
MDP-3A Fails to Start
MDP-3A Fails to Run
Discharge Valve Fails to Open
CCF of Train MDP3A
MDP-3A Unavailable Due to T/M
2.000E-3
6.000E-4
1.000E-6
4.000E-3
MDP-3A Fails to Start
MDP-3A Fails to Restart after Repair
CCF of MDP Trains to Start
CCF of MDP Trains to Start
CCF of MDP Trains to Run
2.000E-3 [TRUE]
7.980E-5 [0.01]
4.410E-6
MDP-3A Fails to Restart
Operator Fails to Repair MDP-3A
CCF of MDP Trains to Start
Operator Fails to Repair MDP-3A
Create simplified CCF subtree with a new logic event
False [2.000E-3]
False [0.1]
7.980E-5 [0.01]
False [0.1]
Create new basic event using nominal FTS probability
Create new recovery event using HRA derived HEP; attach to independent and common cause subtrees

Figure 6-1. An example of sub-tree logic for a repair model added to an existing fault tree. (The basic events in the figure show example base case and change set values).

- ○ The CCF sub-tree is slightly different than the independent failure sub-tree due to simplification. The basic event that represents the nominal CCF probability to restart due to other causes is not modeled for simplicity. This simplistic approach may be slightly non-conservative; however, the CCF contribution during restart is relativity small and developing a new CCF compound event that includes restart can be problematic.
- ○ The recovery event in the CCF sub-tree (*Operator Fails to Repair MDP-3A*) is the same basic event used in the independent failure sub-tree. However, the analyst should consider the specifics of the failure and recovery events to determine whether this duplicative use is appropriate for the analysis.

– *Other details.* Some other details to consider in the above example are as follows:

- ○ The new basic event (*MDP-3A Fails to Restart*) probability can be updated to include recent operating experience as well as the observed failure as one more additional failure. The parameter update would be most important for rare or infrequent failure event. Refer to NUREG/CR-6823 for guidance in parameter estimations.
- ○ For cases involving repair of a FTR event, the modification of the fault tree would be much the same as in the FTS example (replace the FTS-related events to FTR).

The exception is that the FTR basic event parameter for mission time should be reduced to reflect the run time required to complete the remaining sequence mission time (usually 24 hours).

- *Consideration of success terms.* When modifying a fault tree that results in a high failure probability (e.g., 0.1 to 1.0), consult Idaho National Laboratory for guidance on incorporating success terms in the model results. This is especially important for top events with a single basic event for the fault tree.
- *Update the base case SPAR model.* When adding a recovery event to a fault tree, make sure that the base case model is updated, as well as the change case model. Otherwise, a negative cut set importance may be calculated due to a lower core damage probability (CDP) or CDF of the base case SPAR model.
  - For repair actions, the recovery event in the base case model should be set to TRUE or FALSE (no difference) so that the recovery event does not show up in cut sets. Then, the recovery event should be set to the failure -specific HEP in the change case.
  - For recovery actions, the recovery event in the base case model should be set to the failure-specific HEP. No changes should be made to the recovery event in the change case.

6.6 PRA Standard Supporting Requirements– Modeling Recovery

The supporting requirements to the PRA Standard for crediting and modeling recovery and repair actions, including associated index numbers, are provided in this section for reference. For the most part, these supporting requirements apply in an ECA. Questions regarding interpretations and clarifications should be directed to an NRC representative on the ASME Committee on Nuclear Risk Management.

Deviations from or clarifications to the PRA Standard should be justified and documented in the risk analysis.[23]

- ***HLR-HR-H.*** Recovery actions (at the cut set or scenario level) shall be modeled only if it has been demonstrated that the action is plausible and feasible for those scenarios to which they are applied. Estimates of probabilities of failure shall address dependency on prior human failures in the scenario.[24]

- ***HR-H1, Capability Category II.*** Include operator recovery actions that can restore the functions, systems, or components on an as-needed basis to provide a more realistic evaluation of significant accident sequences.

- ***HR-H2.*** Credit operator recovery actions only if, on a plant-specific basis:

[23] Clarifications to the PRA Standard in the Regulatory Guide 1.200 are emphasized in bold italics below.

[24] Recovery actions are actions taken in addition to those normally identified in the review of emergency, abnormal, and system operating procedures, which would normally be addressed in post-initiator HRA (i.e., PRA Standard designators HR-E through HR-G). They are included to allow credit for recovery from failures in cut sets or scenarios when failure to take credit would distort the insights from the risk analysis. The potential for recovery (e.g., manually opening a valve that failed to open automatically) may well differ from scenario to scenario or cut set to cut set. In this context, recovery is associated with work-arounds but does not include repair, which is addressed in SY-A22 and DA-C14.

  - A procedure is available and operator training has included the action as part of crew's training, or justification for the omission is provided.
  - Cues (e.g., alarms) that alert the operator to the recovery action provided procedure, training, or skill of the craft exist.
  - Attention is given to the relevant plant-specific and scenario-specific performance shaping factors provided in HR-G3.
  - There is sufficient manpower to perform the action.

- ***HR-H3.*** Account for any dependency between the HFE for operator recovery and any other HFEs in the sequence, scenario, or cut set to which the recovery is applied (see HR-G7).

- ***HR-G3.*** When estimating human error probabilities, evaluate the impact of the following plant-specific and scenario-specific PSFs:
  - Quality [type (classroom or simulator) and frequency] of the operator training or experience;
  - Quality of the written procedures and administrative controls;
  - Availability of instrumentation needed to take corrective actions;
  - Degree of clarity of the cues/indications *in supporting the detection, diagnosis, and decision-making give the plant-specific and scenario-specific context of the event*;
  - Human-machine interface;
  - Time available and time required to complete the response;
  - Complexity of *detection, diagnosis and decision-making, and executing* the required response;
  - Environment (e.g., lighting, heat, radiation) under which the operator is working;
  - Accessibility of the equipment requiring manipulation; and
  - Necessity, adequacy, and availability of special tools, parts, clothing, etc.

- ***HR-G7.*** For multiple human actions in the same accident sequence or cut set, identified in accordance with supporting requirement QU-C1, assess the degree of dependence, and calculate a joint human error probability that reflects the dependence.[25] Account for the influence of success or failure in preceding human actions and system performance on the human event under consideration including:
  - Time required to complete all actions in relation to the time available to perform the actions;
  - Factors that could lead to dependence (e.g., common instrumentation, common procedures, increased stress, etc.); and
  - Availability of resources (e.g., personnel).

- ***SY-A24.*** Do not model the repair of hardware faults, unless the probability of repair is justified through an adequate analysis or examination of data *collected in accordance with*

[25] The state of the art in HRA is such that the assessment of dependency is largely based on the analyst's judgment.

DA-C15 and estimated in accordance with DA-D9.

- ***DA-C15.*** For each SSC for which repair is to be modeled (as described in SY-A22), identify instances of plant-specific *experience and, when that is insufficient to estimate failure to repair consistent with DA-D9,* applicable industry experience and for each repair, collect the associated repair time with the repair time being the period from identification of the component failure until the component is returned to service.

- ***DA-D9.*** *For each SSC for which repair is to be modeled, estimate, based on the data collected in DA-C15, the probability of failure to repair the SSC in time to prevent core damage as a function of the accident sequence in which the SSC failure appears.*

- ***QU-C1.*** Identify cut sets with multiple HFEs that potentially impact significant accident sequences/cut sets by re-quantifying the PRA model with HEP values set to values that are sufficiently high that the cut sets are not truncated. The final quantification of these post-initiator HFEs may be done at the cut set level or saved sequence level.

6.7 Questions to Consider for Crediting Recovery/Repair Action

A thorough recovery analysis requires careful consideration of the appropriate performance shaping factors in an HRA. Some questions to consider for crediting and modeling the recovery/repair of an observed failure are provided below.

Observations from the actual event can provide insights into the recoverability of a failure. Some questions to consider during the event investigation include:

- How long did the recovery/repair actually take?

- Was there any time pressure for the actual recovery/repair action?

- Were there any difficulties observed during the recovery/repair activity?

- What is the basis for assuming an earlier recovery/repair time than what was actually observed?

- When did the plant staff first determine that the recovery/repair action is plausible and feasible (but decided to defer an immediate action due to operability or availability of redundant SSC)?

- Did a procedure for recovery/repair exist at the time of the event?

- Could the observed failure mechanism result (probabilistically) in a worse case failure that could not be recovered/repaired?

6.8 Considerations for Defining Appropriate Recovery/Repair Actions

The following should be considered in defining appropriate recovery and repair actions:

- Can the failure be recovered/repaired given postulated extreme environmental conditions? Considerations include:

  - High temperatures due to high-energy line break,
  - Flooding from line breaks (e.g., floor drains overfill, overflow down stairways),
  - High radiation levels from sump recirculation,
  - Component accessibility,
  - Chemical hazard (e.g., transformer oil), and
  - Extreme weather (ice, high winds, lightning).

- What are the cues (e.g., alarms) that alert the operator to the need for a recovery action(s) and the failure that needs to be recovered? Will the cues be clear and provided in time for postulated sequences of interest?

- Is there sufficient time for the recovery action(s) to be diagnosed and implemented (repair failure, re-start system, and recover core cooling) to avoid the undesired outcome for postulated sequences? Time-dependent considerations include:
  - Time to core uncovery;
  - Time to recover vessel water level before pressure exceeds pump injection limits [low pressure (pump run-out), high pressure (pump shutoff head)];
  - Time to suppression pool over-pressure failure [BWR only]; and
  - Time to suppression pool temperature exceeding net positive suction head limits [BWR only].

- Can the recovery/repair action be accomplished within the required time frame? Considerations include:
  - Tools readily available,
  - Spare parts readily available,
  - Area lighting and power sources for tools available,
  - Communications with control room available, and
  - Plant staffing level with the right skills.[26]

- Would the crew know how much time is available before core uncovery or other time sensitive considerations?

- Are the crews trained on the recovery action(s) and is the quality and frequency of the training adequate?

- Is there procedural guidance to perform the recovery?

- Is the equipment needed to perform the recovery available in the context of other failures and the initiator for the sequence/cut set? Are the support systems available in sequences in which recovery is credited?

[26] Plant staffing levels during normal plant operations vary during the time of day and day of week. The full complement of the emergency response organization should be activated within 1 hour following the declaration of an emergency (Alert or higher).

This page intentionally left blank.

7.0 Multi-Unit Considerations

7.1 Introduction

At a multiple unit site, an event or condition at one plant unit may have an effect on the other units at the same site. From the standpoint of Management Directive (MD) 8.3, "NRC Incident Investigation Program," event assessment, the total risk impact on all units should be evaluated. If subsequent inspection of the event or condition identified a performance deficiency (PD) that has an effect on more than one unit, then a PD should be written for each affected unit and a Significance Determination Process (SDP) assessment should be performed for each plant unit.

Frequently, multiple units at a given site are connected in order to benefit from pooling their system resources. In general, this turns out to be better than having half the given resources at each of two stand-alone units, but it is not as good as having the total resources unconditionally available to a single unit.

For example, assuming that the cross-tie itself does not introduce significant failure potential, having four service water pumps at two units is better than having two pumps at each of two stand-alone units, but not as good as having four at each of two units. Modeling of this situation needs to address the point that the two units compete for service water resources. If there is plenty to go around, then a simple assumption may be adequate, but if one or more service water pumps fail, the modeling situation can become complex.

Even if two units are not physically connected, their risks may be correlated by virtue of sharing elements of one or more common-cause groups, so that a failure of one element of that group may imply an increased failure potential at both units in the remaining elements.

In general, the challenge to the analyst is not so much to determine if effects exist, because they frequently do, but rather to determine if the effects are significant. Typically, event-induced or condition-induced reductions in the total redundancy of shared systems need careful attention, because they are not always risk-significant but they can be, and it may not be easy to tell without a careful look.

- ***Typical Shared Systems.*** Some systems that can be shared to varying extent at different sites include:
  - Emergency alternating-current (AC) electrical power
    - Emergency diesel generators (EDGs)
    - Station blackout (SBO) diesel generators
    - AC power sources including hydroelectric generators and gas turbine generators
  - Direct-current (DC) electrical power
  - Instrument air and station air,
  - Raw water systems (e.g., service water, emergency service water, emergency equipment cooling water)
  - Component cooling water
  - Auxiliary feedwater (AFW)

  - Condensate storage tank
  - Chemical and volume control

- ***Typical Site-Wide Initiators.*** Examples of event initiators that may impact multiple units include:
  - Loss of offsite power (LOOP)
  - Loss of service water
  - Loss of instrument air (for shared system)
  - Loss of a single AC or DC bus
  - External events including seismic, high wind, and flooding.

7.2 Modeling Considerations

- ***Shared Systems in SPAR Models.*** For the most part, SPAR model fault trees for multi-unit sites already account for shared equipment and systems, as well as crosstie capability as allowed by design and procedures.

- ***Treatment of Shared Assets between Plants****.* If a shared asset only has the capacity to support one plant at a time, then a "shared availability factor" logic event or sub-tree should be incorporated into the system fault tree that reflects the probability that the other plant will not need the asset in order to meet minimal functional success criteria.
  - The shared availability factor should include the frequency of an appropriate dual unit initiator, human error probabilities of implementation actions, and hardware failure probabilities of appropriate failure modes.

- ***Treatment of Operational Events Affecting Multiple Plants at a Site.*** An operational event that impacts more than one plant at a multiple unit site should be evaluated for each plant separately. The results of the risk analysis for each plant should not be added together or integrated into one result.

- ***Windowing.*** In analyzing a given unit, windowing of events, conditions, and maintenance outages on the other unit need to be examined for synergistic implications on the subject unit, including common-cause failure probability changes due to conditions at the other unit, and maintenance-induced limits on the total systems resources available at the site. For example, in a condition analysis of a given unit's AFW pump, knowledge of the other unit's AFW status would be important in an analysis.

- ***Events Affecting only One Unit.*** For events likely to affect only one unit at a time (e.g., general transient, total loss of feedwater flow, steam generator tube rupture, stuck open safety/relief valve, various loss-of-coolant accidents), modeling considerations include the following:
  - It is reasonable to assume that there would be no coincidental event at the other unit(s).
  - Shared equipment, or equipment that can be cross-tied from the unaffected unit, can be credited at the affected unit.
  - Failure to start/run, unavailability for test and maintenance (including when the unaffected plant is in shutdown), and any operator action such as manual crosstie from

the unaffected unit should be modeled appropriately.

- ***Site-Wide LOOP Event.*** For a LOOP initiator affecting the site, modeling considerations include the following:
  - The impact of the event or degraded condition on all units should be assessed (e.g., swing EDG).
  - Two plant units should not take full credit for the same swing equipment at the same time.
  - Carefully review technical specifications and procedures for allowed and disallowed sharing or crosstie configurations.
  - A joint unit analysis may be necessary to ensure that double credit is not taken for shared assets (e.g., a swing EDG).
  - Review procedures to identify if one unit is given clear priority over another (e.g., Millstone Unit 3 has priority over Unit 2 for the SBO diesel generator).
  - Adjust the initiator event frequency based on operating experience to represent site loss. Severe weather-related and grid-related LOOP events are more likely to affect two or more units at a site than a plant-centered LOOP.
  - Support system dependencies such as at Braidwood Unit 1 and 2 (e.g., EDG cooling), whereby one unit’s essential service water may cool the other unit’s EDG by crediting emergency service water crosstie, should be carefully modeled.
  - Consider constructing an aid such as a table or matrix showing all possible combinations of available equipment (e.g., EDGs, alternate AC power, and service water pumps).
  - *Review credit taken for recovery action.* Recovery actions are less probable in a multi-unit LOOP than single-unit LOOP.
  - Carefully review common cause component groups and probabilities.
  - Review cut sets carefully for logical consistency (all dominant cut sets are included; no illogical cut sets are indicated).

- ***Other initiators affecting more than one unit.*** For other initiators potentially affecting more than one unit, proceed in a similar manner to the LOOP case above:
  - Consider the need to adjust the initiator frequency based on operating experience to reflect impact on two or more units.
  - Review relevant system fault trees where operator action to cross-tie units is credited. Ensure the reasonableness of actual plant and operator response to an event (e.g., time available for operator response vs. feasibility of recovery actions under changing environmental conditions).
  - Consider the need to modify value assignments of performance shaping factors in accordance with the human reliability analysis methodology.

7.3 Example of a Multi-Unit SDP Assessment

The example provided below illustrates a SDP assessment of a single performance deficiency (PD) involving inadequate maintenance control at both plants of a two-unit site. The single PD resulted in three degraded conditions, one in Unit 1 and two in Unit 2.

- ***Unit 1 SDP Assessment.*** In Unit 1, a PD was identified which caused a degraded condition by which a random initiating event with subsequent reactor trip would always result in a consequential LOOP. A month after the PD for the degraded condition was introduced in a transformer relay; Unit 1 was at power when it experienced a random reactor trip. The degraded condition resulted in a consequential LOOP that manifested itself through the random reactor trip. Since the PD did not cause the initiating event, the SDP assessment should calculate the change in core damage probability (ΔCDP) in a conditional analysis.[27]

- ***Unit 2 SDP Assessment.*** Unit 2 was shutdown and on shutdown cooling. In addition, electrical power to the operating residual heat removal (RHR) train in Unit 2 was being supplied from Unit 1 via an electrical cross-connection. With the cross-connection, the LOOP event in Unit 1 resulted in a subsequent loss of RHR in Unit 2. The same PD (inadequate maintenance control) impacted Unit 2 in two different ways: (1) the LOOP in Unit 1 resulted in the loss of RHR in Unit 2 and (2) an additional degraded condition (identical to that on Unit 1) was discovered in Unit 2.
  - *Loss of RHR event in Unit 2.* At the time of the LOOP in Unit 1, Unit 2 was in cold shutdown and running on one RHR pump. The RHR pump was being powered from an electrical cross-connection from Unit 1. Therefore, the plant boundary for Unit 2 includes the crosstie up to and including the degraded condition in Unit 1 transformer relay. The PD that caused the LOOP in Unit 1 resulted in the loss of RHR in Unit 2. Given that the Unit 1 LOOP and subsequent loss of RHR manifested itself through the Unit 1 random reactor trip, the SDP should calculate the ΔCDP in a conditional analysis.[28]
  - *Degraded condition in Unit 2.* The same PD was also introduced in Unit 2, which resulted in an additional degraded condition on an identical component and system (transformer relay) in Unit 2. Like Unit 1, the degraded condition in Unit 2 would always result in a concurrent LOOP given a random reactor trip of Unit 2 (during at-power operations). Given that no random reactor trip was involved in Unit 2, the SDP should calculate the ΔCDP in a conditional analysis.[29]
  - *Number of findings in Unit 2.* The PD impacted Unit 2 at two different time periods: (1) the degraded condition over the one-month exposure time prior to shutdown and (2) the loss of RHR initiating event during shutdown. Since the same PD impacted Unit 2 at two different time periods that were not overlapping, the risk impacts are additive. Thus, one finding for Unit 2 is appropriate because the PD is the same.[30]

[27] MD 8.3 and ASP analyses would calculate the conditional core damage probability (CCDP) for the LOOP event in an initiating event analysis, since the identification of a PD is not required for MD 8.3 and ASP analyses.

[28] MD 8.3and ASP analyses would calculate the CCDP for the loss of RHR event in a shutdown initiating event analysis, since the identification of a PD is not required for MD 8.3 and ASP analyses.

[29] MD 8.3 and ASP analyses would also calculate the ΔCDP of the potential of a LOOP given a postulated random reactor trip in a conditional analysis.

[30] MD 8.3 and ASP analyses would also combine the risk associated with the initiating event and degraded condition using the guidance in Section 8.

Figures 7-1a and 7-1b show the core damage probability (CDP) versus time and core damage frequency (CDF) versus time for Unit 2 (SDP assessment only).

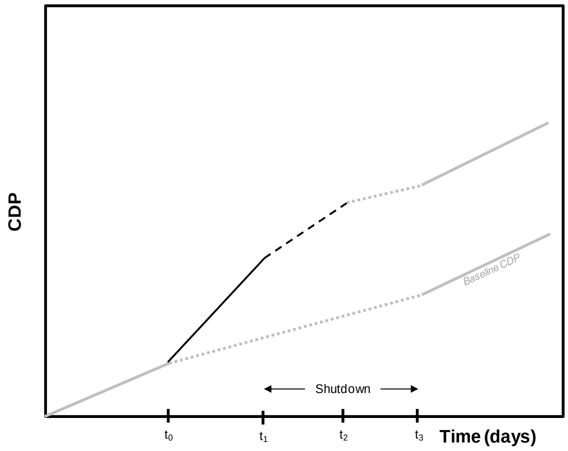


Figure 7-1a. CDP vs. time for example (Unit 2).

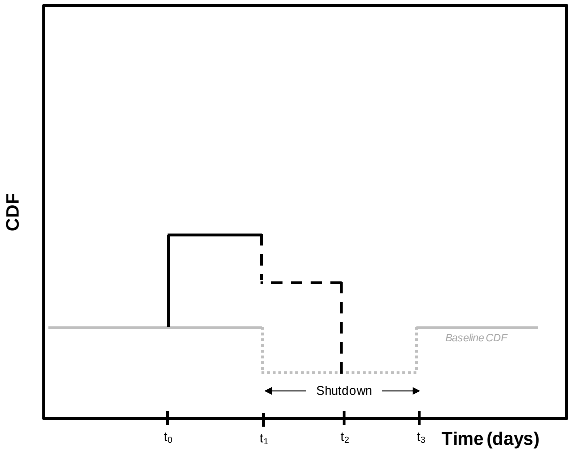


Figure 7-1b. CDF vs. time for example (Unit 2).

An explanation of the key aspects of Figures 7-1a and 7-1b are provided below:

t_0 The PD causes an at-power degraded condition for Unit 2.

$t_0 – t_1$ An increase in the Unit 2 CDP due to the at-power degraded condition in Unit 2 (solid black line). A random reactor trip in Unit 2 can result in a consequential LOOP in Unit 2.

t_1 Unit 2 enters shutdown operations. The Unit 2 operating RHR pump is now powered from Unit 1 via an electrical cross-connect. A random reactor trip in Unit 1 can now result in a loss of RHR in Unit 2.

$t_1 – t_2$ An increase in the Unit 2 shutdown CDP occurs due to the at-power degraded condition in Unit 1 with the Unit 2 operating RHR Pump being powered from Unit 1 (dashed black line). The slope of this line is less than the slope of the at-power condition (solid black line) because risk is assumed to be lower during shutdown.

t_2 A random reactor trip in Unit 1 in combination with the PD leads to a consequential LOOP in Unit 1 resulting in the subsequent loss of RHR in Unit 2. The Unit 1 and Unit 2 degraded conditions are identified and corrected during day t_2.

$t_2 – t_3$ Unit 2 remains in shutdown operations with no degraded conditions (dotted grey line). The slope of this line is the same as the baseline shutdown line.

t_3 Unit 2 begins at-power operations (solid grey line). The slope of this line is the same as the baseline at-power line.

This page intentionally left blank.

8.0 Initiating Events Analyses

8.1 Objective and Scope

- ***Objective.*** This section provides guidance on the treatment of initiating events during at-power operation in event and condition assessments (ECAs). This section discusses the treatment of initiating events with and without availability of a structure, system, or component (SSC). The cause of an observed SSC unavailability and/or observed initiating event must be associated with the same performance deficiency (PD) for a Significance Determination Process (SDP) evaluation. The identification of a PD is not required for an Accident Sequence Precursor (ASP) or Management Directive (MD) 8.3, "NRC Incident Investigation Program" assessments.

  Guidance provided in this section does not change the guidance provided in Appendix A of this volume of the handbook for ASP and MD 8.3 assessments of initiating events. The treatment of initiating events in SDP evaluations have been applied in the past for certain performance deficiencies associated with at-power findings, although infrequently (as expected).

- ***In Scope.*** Treatment cases that are in the scope of this guide are summarized below.[31]
  - *Case 1– Initiating event only.* A PD causes an initiating event with subsequent reactor trip and the same PD does not cause other complications.
  - *Case 2– Initiating event and mutually exclusive SSC (SDP only).*[32] A PD causes an initiating event with subsequent reactor trip and the same PD causes an observed unavailability of a SSC that is mutually exclusive of the initiating event.
  - *Case 3– Initiating event and mutually inclusive SSC.* A PD causes an initiating event with subsequent reactor trip and the same PD causes an observed unavailability of a SSC that is mutually inclusive of the initiating event.
  - *Case 4– SSC unavailability increases the initiating event frequency.* A PD results in a degraded or unavailable SSC that could increase the frequency of an initiating event; however, no reactor trip occurred (e.g., failure of a single service water pump).

- ***Not in Scope.*** The following cases below are outside the scope of this guide.
  - A PD that did not cause a reactor trip occurrence or SSC unavailability, but created a degraded condition that could increase the frequency of an initiating event (e.g., excessive pipe wall thinning without loss of function).
  - A PD that did not cause a reactor trip, but contributed to a consequential initiating event (e.g., loss of offsite power event) given a random reactor trip. Such cases are evaluated in SDP as a condition analysis. See Appendix A of this volume of the handbook for guidance on condition analyses.

[31] The identification of a PD noted in each case below is required for a SDP analysis, but is not required for ASP and MD 8.3 analyses. ASP and MD 8.3 only requires the observation of a SSC unavailability and/or reactor trip.

[32] This case only applies for SDP evaluations.

8.2 Case 1– Initiating Event Only

For this case, a PD causes an initiating event with subsequent reactor trip. In addition, the same PD did not affect any SSCs or cause other complications during the initiating event. This case involves one calculation—a conditional core damage probability (CCDP) estimation associated with the reactor trip (i.e., an initiating event analysis). For ASP and MD 8.3 analyses, a PD does not have to be identified or associated with the initiating event.

- ***Consider Adjustments to Test and Maintenance (T/M) Basic Events (ASP and MD 8.3 only).***[33] For ASP and MD 8.3 analyses, a SSC that was unavailable due to T/M at the time of the initiating event is modeled as unavailable; therefore, the associated T/M basic event is set to TRUE. Potential recovery actions for restoring the SSC should be modeled, as appropriate. Refer to the Section 6 on modeling recovery for additional information.

- ***Calculate CCDP.*** Calculate the CCDP by setting the observed initiating event (e.g., general transient, loss of main feedwater, loss of vital bus transient) to 1.0 and all other initiating events to 0.0.[34]
  - For SDP evaluations, multiply the CCDP by one inverse year (yr^{-1}) to equate this to a change in average core damage frequency (ΔCDF_{ave}).
  - For ASP and MD 8.3 analyses, the final metric is the CCDP.

Figure 8-1a and Figure 8-1b provide the core damage probability (CDP) versus time and core damage frequency (CDF) versus time for Case 1.

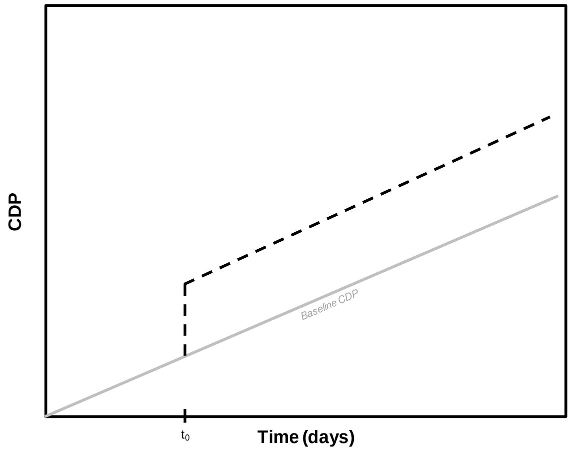


Figure 8-1a. CDP vs. time for Case 1.

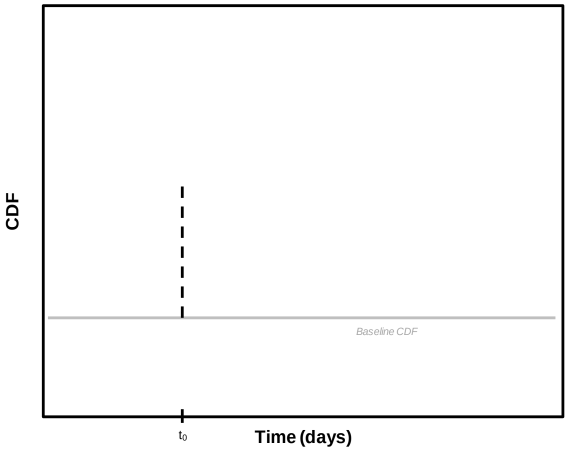


Figure 8-1b. CDF vs. time for Case 1.

The plot of CDP vs. time (Figure 8-1a) shows a line[35] representing the CDP vs. time prior to the initiating event, at t_0 a "spike" in CDP accumulates due to an initiating event with subsequent reactor trip, and then the CDP returns to the same slope as the baseline CDP following the

[33] For SDP evaluations, the T/M basic events remain unchanged at their nominal unavailability probabilities, given that observed unavailability due to T/M was not related to the identified PD.

[34] If using the SAPHIRE General Analysis Module use TRUE/FALSE instead of 1.0/0.0.

[35] In the CDP vs. time plots, the slope of the line is equal to the CDF.

initiating event (t_0).[36] A plot of CDF vs. time (Figure 8-1b) shows a horizontal line (equal to the baseline CDF), with Dirac delta function (or “spike”) at t_0 when the reactor trip occurs. After the initiating event occurs, the CDF returns to equal the baseline CDF. The CDP is approximately the integral of CDF over time. At the point where the initiating event occurs (t_0), the integral is equal to the CCDP multiplied by the integral of the delta function, which is numerically equal to the CCDP.

8.3 Case 2– Initiating Event and Mutually Exclusive SSC Unavailability (SDP Only)

For this case, a PD causes an initiating event with subsequent reactor trip. In addition, the same PD also causes an unavailability of a SSC that was mutually exclusive of the initiating event. The exposure time of the unavailable SSC may sometimes overlap with the time of the observed reactor trip event. However, the unavailable SSC is not required for mitigation of any of the initiating event sequences. This case only applies for SDP evaluations.[37]

Case 2 involves three calculations: (1) CCDP estimation (initiating event analysis) associated with just the initiating event, (2) ΔCDP estimation (condition analysis) associated with just the SSC unavailability over the exposure time, and (3) the sum of the CCDP and ΔCDP results.

- ***Calculate CCDP for the Initiating Event.*** Calculate the CCDP by setting the observed initiating event (e.g., general transient, loss of main feedwater, loss of vital bus) to 1.0 and all other initiating events to 0.0.[38] Numerically, this is equivalent to a change in average CDF (ΔCDF_{ave}) over one year when CCDP is divided by one year.

- ***Calculate ΔCDP for the SSC Unavailability.*** In a condition analysis, the basic event associated with the SSC unavailability is set to TRUE and the SPAR model is solved to calculate the ΔCDP over the exposure time. Do not adjust any initiating event frequency in this step of the SDP evaluation. Potential recovery action for restoring the SSC (see Section 6) and adjustments to T/M basic events (see Section 8.2) may be considered, as appropriate.

  The SSC unavailability causes an increase in the CDF that lasts for a specified period of time, Δ*t*. The ΔCDP is calculated as

$$\Delta CDP = (CDF_{new} - CDF_{base}) \times \Delta t$$

Ensure that the units of time match with the terms in this equation. Numerically, this is equivalent to a change in average CDF (ΔCDF_{ave}) over one year when ΔCDP is divided by one year.

- ***Calculate Total R*isk (ΔCDF$_{ave}$).** Calculate the total ΔCDP by adding together the CCDP for the initiating event and the ΔCDP for the SSC unavailability. The result is:

[36] This plot assumes the reactor was returned to at-power operations at t_0; therefore, showing no change in the lower baseline CDP line. Had the reactor remained in shutdown for a given period, the slope of the baseline CDP would change during this period. The slope of the upper line would track the shutdown baseline over the shutdown period.

[37] This case only applies for SDP evaluations. MD 8.3 or ASP analysis requires a SSC failure to occur during (concurrent with) the initiator’s PRA mission time (generally within 24 hours following the reactor trip).

[38] If using the SAPHIRE General Analysis Module use TRUE/FALSE instead of 1.0/0.0.

$$\Delta CDP_{Total} = CCDP + (CDF_{new} - CDF_{base}) \times \Delta t$$

Multiply the ΔCDP_{Total} by one inverse year (yr^{-1}) to equate this to a change in average core damage frequency (ΔCDF_{ave}).

Figure 8-2a and Figure 8-2b provide the CDP versus time and CDF versus time for Case 2. From t_0 to t_1 Case 2 is identical to Case 1; however, the same PD that caused an initiating event with subsequent reactor trip at t_0 also caused an unavailable SSC from t_1 to t_2 (i.e., Δt). The unavailable SSC is restored at t_2.

The plot of CDP vs. time (Figure 8-2a) shows the CDP spike at t_0 due to the initiating event with subsequent reactor trip and CDP returning to the same slope as the baseline CDP following the initiating event (as in Case 1).

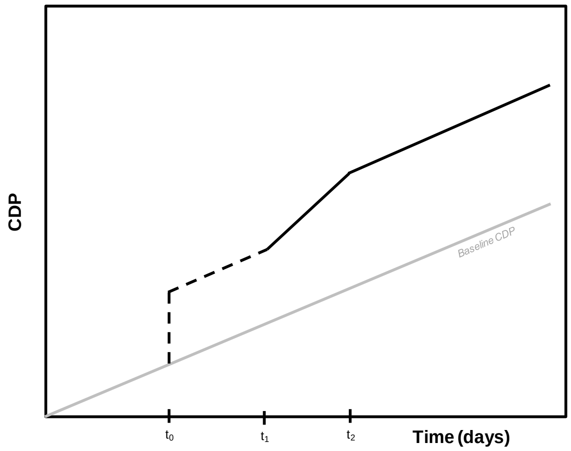


Figure 8-2a. CDP vs. time for Case 2.

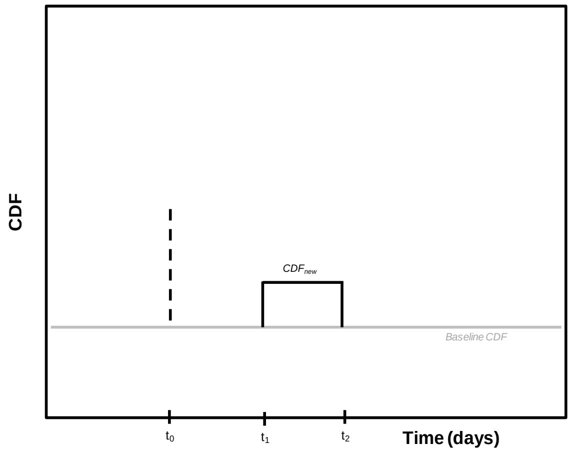


Figure 8-2b. CDF vs. time for Case 2.

At t_1 the PD caused the unavailability of a SSC; therefore, the CDP slope increases, and then the CDP returns to the same slope as the baseline CDP when the condition is corrected at t_2. The plot of CDF vs. time (Figure 8-2b) shows a horizontal line equal to baseline CDF (i.e., CDF_{base}) with a "spike" occurring at t_0 due to the initiating event with subsequent reactor trip. The CDP then jumps to a higher horizontal line (CDF_{new}) from t_1 to t_2, due to the unavailable SSC. The ΔCDP is approximately the integral of CDF over time.

These plots show an example of Case 2 where the initiating event and condition do not overlap, and the deficiencies associated with the initiating event and condition were fixed at different times (t_0 and t_2, respectively). Other variations of this case are possible, such as the condition starting at a sometime before the reactor trip and fixed sometime after the reactor trip.

8.4 Case 3– Initiating Event and Mutually Inclusive SSC Unavailability

For this case, a PD causes an initiating event with subsequent reactor trip. In addition, the same PD causes an observed unavailability of a SSC that was mutually inclusive of the initiating event. The observed unavailability must overlap with the observed reactor trip event and the unavailable SSC must be required for mitigation of any of the initiating event sequence(s). For ASP and MD 8.3 analyses, a PD does not have to be identified or associated with the initiating event and/or SSC unavailability.

This case involves the comparison of two calculations: (1) CCDP estimation (initiating event analysis) associated with the combined initiating event and SSC failure, and (2) ΔCDP estimation (condition analysis) associated with just the SSC unavailability over the exposure time. To avoid double counting, the highest result of the two calculations is documented for the record.

- ***Calculate CCDP for the Combined Initiating Event and SSC Unavailability.*** The calculation of CCDP may differ slightly between a SDP evaluation and MD 8.3 or ASP analysis. The SDP evaluation considers both the initiating event and SSC unavailability in the same initiating event analysis only if the same PD was involved. ASP and MD 8.3 analysis consider all failures that were observed during the initiating event, regardless of an identified or common PD.
  - For SDP evaluations, follow the same guidance in Section 8.2 to calculate the CCDP associated with the initiating event. In the same calculation, set the basic event associated with the SSC unavailability to TRUE. Model potential recovery actions for restoring the SSC, as appropriate. Refer to the Section 6 on modeling recovery for additional information.
  - For ASP and MD 8.3 analysis, follow the same guidance in Section 8.2 to estimate the CCDP associated with the initiating event. In addition, set the basic event associated with the SSC unavailability to TRUE and set any other observed equipment failures to TRUE. Consider adjustments to T/M basic events as appropriate. Model potential recovery actions for restoring the SSC, as appropriate. Refer to the Section 6 on modeling recovery for additional information.

- ***Calculate ΔCDP for the SSC Unavailability Only.*** For SDP, ASP, and MD 8.3 analyses, follow the same guidance in Section 8.3 to estimate the ΔCDP associated with the SSC unavailability over the exposure time. Do not include the initiating event in this step of the calculation. Model potential recovery actions for restoring the SSC, as appropriate. Refer to the Section 6 on modeling recovery for additional information.

- ***Choose the Highest of the CCDP or ΔCDP Result.*** Given that both calculations include the risk contribution of the SSC failure (or unavailability); only the highest result should be recorded as the final result.

8.5 Case 4– SSC Unavailability Increases the Initiating Event Frequency, but No Initiating Event Occurred

For this case, a PD results in an observed unavailability of a SSC that could increase the frequency of an initiating event; however, no initiating event occurs. Certain equipment failures, particularly for SSCs in support systems (e.g., service water, component cooling water, instrument air) can lead to an increase in the system failure probability. If a system failure can result in an initiating event, then an increase in system failure probability can increase the initiating event frequency, in addition to an increase in the overall plant risk due to the reduction in mitigation capability.

One approach to estimate the change in initiating event frequency for a condition that involved the failure of an SSC but did not result in an initiating event is provided as follows.
Plant-specific support system initiating event (SSIE) models in SPAR models should support an

alternate method of handling the increase in initiating event frequency due to a failed support system SSC. Section 11 provides guidance for the use of the SSIE models in ECA.

- ***Solve the Applicable Fault Tree in the SPAR Model***. This provides an estimate of the baseline system failure probability.

- ***Calculate the System Failure Probability Factor***. Use a change set in Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) to model the observed component failure (set the basic event to TRUE) and solve the system fault tree to obtain the modified system failure probability. Calculate the system failure probability factor (or ratio) by dividing the baseline system failure probability into the modified system failure probability.

- ***Calculate the Modified Initiating Event Frequency.*** Multiply system failure probability factor with the baseline initiating event frequency to calculate the new initiating event frequency.

- ***Consider Recovery Actions.*** Recovery actions to restore the loss of function due to the SSC failure may require prompt corrective actions in order to prevent an automatic or manual reactor trip. Special attention to the timing of the initiating event and complexity of the associated recovery action should be considered in the human reliability analysis of the nonrecovery probability. Refer to the Section 6 on modeling recovery for additional information.

- ***Calculate ∆CDP for Degraded Condition.*** Solve the SPAR model with the modified initiating event frequency and the SSC unavailability (set to TRUE) to obtain the ∆CDP for the overall condition. Follow the same guidance in Section 8.3 to estimate the ∆CDP associated with the SSC unavailability over the exposure time.

8.6 Other Considerations

Additional considerations are provided below.

- In ASP and MD 8.3 analyses, all unavailable SSCs that overlap a reactor trip event are evaluated in one risk assessment.

- In the SDP, a PD that caused an initiating event with subsequent reactor trip will be evaluated separately from other performance deficiencies revealed during the event. The guidance of Inspection Manual Chapter (IMC) 0609, “Significance Determination Process,” and IMC 0308, “Reactor Oversight Process Basis Document,” apply to defining PDs.

- This section does not address recovery of functions lost as a result of the initiating event such as main feedwater or service water. Refer to the Section 6 on modeling recovery for additional information.

- For SDP evaluations, the analyst may need to consider whether the PD that directly caused an initiating event with subsequent reactor trip also represented a degraded condition over a defined exposure period. In these cases, the analyst may need to determine which analysis approach best represents the effects of the PD. An alternative analysis approach can be presented as a sensitivity evaluation.

- A Bayesian update of the initiating event frequency using the observed initiating event over a duration time period should not be used for treatment of initiating events in ECA. The reason is that we are trying to estimate the risk significance of the actual occurrence of an event caused by a deficiency, and the Bayesian update produces a change in the initiator frequency that reflects the occurrence of the initiator over some period of time, which is a different calculation. Furthermore, a Bayesian update assumes that the prior distribution and the plant-specific data are consistent; the fact that the initiating event was caused by a deficiency, which is assumed to cause a significant increase in the frequency of the initiator, invalidates this assumption.

This page intentionally left blank.

Methods Guide: Human Reliability Analysis	Section 9

9.0 Human Reliability Analysis

9.1 Purpose

The purpose of this guide is to address the application of Human Reliability Analysis (HRA) methods in Significance Determination Process (SDP), Accident Sequence Precursor (ASP), or Management Directive (MD) 8.3, “NRC Incident Investigation Program,” assessments. These applications require the analysts to perform analyses of sufficient quality to support regulatory decision making in Reactor Oversight Process (ROP) and Incident Response activities within the timeframe allotted under those processes. The HRA guidance presented here provides best practices of HRA to enable the NRC staff to make timely decisions whose quality is adequate for those processes. However, this guidance may not constitute acceptable positions in all regulatory applications (e.g., license amendment requests). In the development of this guidance, the staff has referred to various sections of reports issued by the NRC, national laboratories, and industry to present best practices that would result in realistic results and enable achieving technical consistency and stability of regulatory decisions. However, this strategy does not constitute unconditional endorsement of those references for all regulatory applications.

Basic events representing human actions required to mitigate initiating events are contained in the SPAR models and are typically quantified using NUREG/CR-6883,” SPAR-H Human Reliability Analysis Method.” An analyst may need to re-quantify a human failure event (HFE) already contained in the model and/or the analyst may need to add an HFE(s) based on the specifics of the risk analysis.[39]

In light of the importance of operator actions on the risk significance of shutdown events, the analyst should consult with an HRA expert and document the technical basis for adding the HFE [if an analyst decides to add new HFE(s)].[40]

9.2 Key Aspects of the SPAR-H Method

- ***Background.*** To ensure consistency, if the HFE is already defined and modeled in the applicable SPAR model for an event assessment (e.g., SDP, ASP, and MD 8.3), the SPAR-H method should be used to quantify the human error probability (HEP). Other HRA methods used to quantify HEPs may be used as sensitivity analyses. The SPAR-H framework decomposes the human error probability into contributions from diagnosis failures and action failures. In addition, the SPAR-H quantification process accounts for the influence of eight performance shaping factors (PSFs).

  In 2011, INL/EXT-10-18533, “SPAR-H Step-by-Step Guidance,” was developed to provide guidance for analysts when plant-specific information is available (e.g., during event and

[39] A HFE is defined as a basic event that represents a failure or unavailability of a component, system, or function that is caused by human inaction, or inappropriate action.

[40] An HRA expert should have training and experience with the particular application of the HRA method being used. Definition is referenced from NUREG-1489, “A Review of NRC Staff Uses of PRA.”

condition assessments), which supplements the general guidance provided in the NUREG/CR-6883. A brief summary of the key steps of using SPAR-H are provided below.

- ***Step 1: Categorizing the HFE as diagnosis and/or action.*** In the context of SPAR-H, HFEs are categorized as either Diagnosis tasks or Action tasks or combined Diagnosis and Action. Diagnosis for the purpose of SPAR-H quantification refers to the entire spectrum of cognitive processing, from the very complex process of interpreting information and formulating an understanding of an upset situation, to the very simple process of just deciding to act and how to act (i.e., deciding which procedure(s) and/or procedure steps to use). Most HFEs in the SPAR models involve much more cognition than merely an action of pushing a switch; therefore, it is not appropriate to routinely exclude the Diagnosis component from HFE quantification. This is consistent with the guidance provided in NUREG-1792, “Good Practices for Implementing Human Reliability Analysis.”

- ***Step 2: Evaluate the PSFs.*** Once the HFE has been characterized as Diagnostic and/or Action, the analyst, as part of the supporting qualitative analysis, must identify the salient performance drivers, both positive and negative. This can be supported by reviewing the eight SPAR-H PSFs. Each PSF needs to be examined with respect to the context of the HFE to resolve two basic issues. First, is there adequate information to judge the influence of the PSF? Second, does the context for that PSF exert a significant influence on the likelihood of failure for the human operator (i.e., is the PSF a “performance driver”)? Only those PSFs that have sufficient information to allow an informed judgment and have been identified as performance drivers should then be evaluated and quantified. Otherwise, the PSF should be assumed to be nominal. The eight PSFs in the SPAR-H method are:

  – Available Time

  – Stress/Stressors

  – Complexity

  – Experience/Training

  – Procedures

  – Ergonomics/Human-Machine Interface

  – Fitness for Duty

  – Work Processes

  INL/EXT-10-18533 provides detailed information on how an analyst should assign the appropriate PSF level once a particular PSF is determined to be a “performance driver.” In addition, an analyst should only include assessment of multiple PSFs if there is reason to believe that each of the respective PSFs is a separate performance driver in its own right, and not merely as a side effect of one of the other PSFs (i.e., “double counting”).[41]

- ***Step 3: Calculate PSF-Modified HEP.*** Once the PSFs levels have been assigned, then the final HEP is simply the product of the nominal HEP and the PSF multipliers. When Diagnosis and Action are combined into a single HFE, the two HEPs are calculated

[41] Double-counting refers to an analyst adjusting more than one PSF based on a single performance driver. For example, an analyst could consider that poor procedures would increase the complexity of an operator action; and therefore, both the Procedures and Complexity PSFs should be adjusted. However, this would be incorrect and is an example of double counting. Only one PSF should be adjusted for each identified performance driver. In this example, only the Procedures PSF should be adjusted to account for the poor procedures.

separately and then summed to produce the composite HEP. Mathematically, it is possible to have a value exceeding 1.0; however, if the two probabilities are small, then the rare-event approximation (i.e., the simple arithmetic sum) is acceptable. In the event that a combined Diagnosis and Action HEP approaches or exceeds 1.0, the following equation should be applied:

$$HEP = \frac{NHEP \times PSF_{composite}}{NHEP \times \left(PSF_{composite} - 1\right) + 1}$$

where *NHEP* is the respective nominal HEP for Diagnosis and Action and $PSF_{composite}$ is the product of the PSF level multipliers. This formula will ensure that the individual Diagnosis and Action HEP values do not exceed a probability limit of 1.0.

9.3 Minimum HEP for Single HFE

In past applications of HRA in general, and SPAR-H in particular, questions have arisen concerning extremely small HEPs. When HEPs are evaluated to be in the 10^{-6} range (literally, one in a million), failure mechanisms that would otherwise be judged to be insignificant contributors to the total failure probability and consequently could be ignored, now become relatively important contributors that need to be included in the HEP estimate.

For situations where there is extensive time available or other extenuating circumstances that would support a very low HEP, the validity of very low probabilities would require estimating the likelihood of the operators committing an error that was simply not recoverable. The concern then is not one of given enough time, surely the operators would eventually get it right, but what is the chance that a mistake is made that prevents further efforts at getting it right? The accident at Three Mile Island is an example where many hours were available but mistakes were still made. Empirical evidence suggests that HEPs in such a low range can only be associated with highly repetitive, highly skilled actions.

In order to ensure consistent implementation of SDP, ASP, and MD 8.3 analyses, the minimum HEP (i.e., lower bound) for a single HFE is 10^{-5}. NUREG-1792 states that "typical post-initiator HEPs are expected to be in the range of 0.1 to 10^{-4})."[42] In the event the analyst concludes that use of the lower bound 10^{-5} leads to overly conservative conclusion, document the technical basis for deviating from the lower bound and have it validated by an HRA expert. Criteria that can justify a single HEP as low as 10^{-6} (as suggested by EPRI Report 1021081, "Establishing Minimum Acceptable Values for Probabilities of Human Failure Events: Practical Guidance for PRA,") are as follows:[43]

- Well-practiced,
- Familiar responses with expansive time to respond,
- Numerous indications (cues) of the need for action,

[42] INL/EXT-10-18533 on the partitioning the *Time Available* PSF between Diagnosis and Action component of a HFE (specifically, the setting of the *Time Available* for Action to nominal) will typically limit the calculated HEP to 10^{-3}. While this may be appropriate for most at-power situations, lower HEPs are possible for HFEs for which very long time periods are available (e.g., shutdown HFEs, containment venting, refilling reactor water storage tank, etc.). Future modifications of the SPAR-H method may be needed to address this issue.

[43] For this lower bound to be applicable, all criteria must be present and clearly documentable.

  - Procedural guidance and training that leads to monitoring of plant status to assess the efficacy of response, thus allowing opportunity for self-correction, and
  - Low workload (i.e., no distractions).

9.4 Analysis of Dependencies

- ***Determination of Dependency.*** Simply stated, dependence may exist when factors that contribute to the occurrence of one HFE may affect the likelihood of a second HFE. Dependence at the HFE level occurs when operators have an incorrect mental model about the situation (or diagnosis of the event) and that incorrect mental model persists across time. Therefore, as dependence arises from operator mindset, the key to postulating dependence between human actions is postulating a single mindset that spans HFEs. Simply having two or more HFEs together in a sequence or cut set does not make them dependent.

  It is expected that the qualitative analysis and resulting context and operational story should help to identify the existence of compelling reasons for dependence. The analyst should be on the lookout for situations in which operators develop an incorrect mindset about the situation and identify ways in which that mindset can be corrected to break dependence. Analysts should review the situation and context carefully and consider, for example, the following factors allow for an opportunity to minimize or break dependence:

  - Time (to allow forgetting and emptying of working memory). The analyst must consider time available to implement recovery actions against the time required to determine the influence of this factor on dependency. For example, whereas ten minutes may have no impact, one or more shift turnovers may have a significant influence on dependency.
  - Location (introducing new information, potentially interrupting the erroneous mindset),
  - Different persons or crew (allows for new mindset to develop), and
  - Cues (stimulate the human to think differently).

  Some compelling reasons that can cause dependence (this list is not exhaustive):

  - No feedback,
  - Misleading feedback,
  - Masking of symptoms,
  - Disbelieving indications,
  - Incorrect situation assessment or understanding of the event in progress,
  - Situation mimics an often-experienced sequence,
  - Situation triggers a well-rehearsed, well-practiced response,
  - Time demand, workload, and task complexity (such that a slip, lapse, or mistake is more likely), and
  - Multiple actions relying on the cues or diagnoses.

- ***Accounting for Dependence.*** In PRA and HRA, dependence can be accounted for in the following ways.

  - *Common PSF Adjustment.* One method of accounting for dependence is through common PSF adjustments of multiple HFEs. If training is poor, stress is high, or available time is short, multiple HFEs could be affected, and this dependence is accounted for by adjusting the appropriate PSFs for each affected HFE. However, there are other potential causes of dependence that are not accounted for via the SPAR-H PSFs but which might still need to be included in the final quantification of two or more HFEs in the same sequence or cut set.

– *THERP Dependency Table.* In determining the level (i.e., degree) of dependence, SPAR-H adapts from Technique for Human Error Rate Prediction (THERP) the factors of same person/crew, close/not-close in time, same/different location, and presence/absence of additional cues.[44] SPAR-H also adapts the same dependence levels used in THERP: zero, low, moderate, high, and complete. The dependence level table in SPAR-H was designed to identify situations in which there is likely to be unchanged mindsets. In order to maintain consistent application of guidance, the analysts should document the basis and/or assumptions for deviations. If such deviations are likely to contribute to significant regulatory outcomes, the analyst should request an independent validation of the assumptions by an HRA expert.

– *Apply a Joint HEP for multiple HFEs.* In sequences or cut sets where more than one HFE exists, the analyst may determine that the value for the combined HEPs should be limited by a lower bound value due dependencies that are not currently accounted for in the HEP calculations of the HFEs. The HRA Good Practices (NUREG-1792) recommends a joint HEP lower bound of 10^{-5} for cut sets containing more than one HFE. After conferring with the authors of NUREG-1792, the lower bound was motivated principally by concerns about dependence among HFEs in a cut set and was included to ensure that analysts consider dependence between HFEs in a cut set. It is permissible that a joint HEP be lower than 10^{-5} if there is a good basis for little or no dependence among the HFEs appearing in the sequence or cut set.[45]

  EPRI Report 1021081 provides a more detailed approach in determining the level of dependence between HFEs and applying minimum joint probabilities. Based on the determination of the level of dependence, an analyst will assign a joint HEP of 10^{-5} (low dependence) or 10^{-6} (very low dependence).[46] In addition, the report states that, “if the criteria for independent HFEs are met, it should not be necessary to employ an alternative minimum value rather than the one calculated.”

  Some of the key factors in determining dependence described in EPRI Report 1021081 are:

  ○ Are the HFEs related to the same critical safety function?

  ○ The amount of time that separates the actions.

  ○ The level of operator workload.

[44] THERP is documented in NUREG/CR-1278, “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.”

[45] EPRI Report 1021081 states, “Using a minimum value of 10^{-5} has resulted in findings that would otherwise have characterized an event or condition as having very low risk becoming White findings. Therefore, while it might be reasonable to adopt some sort of limit, it needs to be done carefully, so that the results of PRAs are not distorted by arbitrary assignments of probabilities. As discussed in detail later on, any limiting values should be consistent within the context of the scenarios in which they are applied.

[46] A minimum joint HEP is not expected to be needed if HFEs are determined to have moderate or high dependence because the product of their individual HEPs is expected to be much higher than 10^{-5}.

- ○ The quality of instrumentation and procedures.
- ○ Is the need for each HFE indicated by separate/multiple cues?
- ○ Is the crew and plant being monitored independently by the shift supervisor and/or shift technical assistant?

Additional details on determining the level of dependence between HFEs and the associated minimum HEP (if applicable) are provided in Section 4 of EPRI Report 1021081.

– *SDP-Specific Guidance.* In order to minimize the subjectivity in SDP analyses, an analyst must consult an HRA expert if it is determined that a minimum joint HEP of lower than 10^{-5} is used. Some questions that the analyst must discuss with the HRA expert prior to determining whether a minimum joint HEP 10^{-6} can be used are:

  - ○ What are the differences in indications among the HFEs? Do those indications bring in new information?
  - ○ Was there a turnover in shift (meaning is the time to perform both actions longer than at least one shift's duration)?
  - ○ Were there successes that are indicative of "resetting" of mindsets on the operators?
  - ○ How much time is available?
  - ○ What is the distribution of workload among operating crew for the different HFEs?

An analyst should not use a minimum joint HEP of less 10^{-6} for SDP analyses. Therefore, a SDP analysis always assumes some level of dependence between HFEs even if the specific reason for that dependence cannot be identified.

Methods Guide: Loss of Offsite Power Initiating Events | Section 10

10. Loss of Offsite Power Initiating Events

10.1 Purpose

This section provides guidance for risk analysis of total loss of offsite power (LOOP) initiating events. This guide supplements the guidance provided in Appendix A of this handbook. The guidance provided in this section is primarily for Management Directive (MD) 8.3, “NRC Incident Investigation Program,” and Accident Sequenced Precursor (ASP) assessments.

10.2 Scope

In-Scope. The scope of this guide includes analysis of initiating events involving a total LOOP event that precedes or results in subsequent automatic or manual reactor trip. A total LOOP event is defined as loss of offsite power supply to all safety-related (or vital) buses where manual operator action was required to restore offsite power to all safety-related alternating-current (AC) buses.

Not In-Scope. Events that are outside the scope of this guide include:

- SDP analysis of a LOOP in accordance with the guidance provide in Section 8. Although, some of the guidance provided in this present section could apply to a SDP analysis, careful considerations of program difference are required when applying this section in SDP.

- Partial LOOP event involving loss of power supply to one or more, but not all safety-related AC buses.

- Total LOOP to all safety buses with no automatic or manual reactor trip. The plant continues generation of electrical power due to the availability of offsite power supply to balance-of-plant (BOP) loads. For example, a fault in a feeder transformer results in a LOOP to safety buses, but not to BOP buses due to decoupled electrical distribution arrangements. Information typically needed for the analysis of total LOOP events are provided in Table 10-1 (located at the end of this section).

10.3 Scenario Definition

As discussed in this guide, the loss of offsite power scenario includes a reactor trip with a loss of offsite power to all safety-related AC buses. In addition, the scenario may include one or more of the following characteristics:

- Offsite power to BOP loads (buses) may have been lost (e.g., successful fast transfer to an alternate offsite power source).

- Standby emergency power sources [e.g., emergency diesel generators (EDGs)] started and loaded onto the designated safety buses.

- One or more emergency power sources may have failed to run for its entire mission time.[47]

- Offsite power may be readily available to be reconnected to one or more safety-related AC buses.

- Recovery of offsite power to one or more safety buses may take many hours even with offsite power readily available and recoverable from the control room.

- Extent of the electrical fault not initially known (typical for plant-centered LOOP events) or the cause of the LOOP event may be initially known (e.g., caused by a known maintenance activity).

10.4 LOOP Recovery Models

Two recovery analysis methods are presented below that estimates LOOP nonrecovery probabilities for the various recovery times used in the LOOP and station blackout (SBO) event trees.

- The SPAR-H method is generally used when event details are known about an actual LOOP event. A benefit of a detailed recovery analysis using a human reliability analysis (HRA) method is to address possible operator actions in a reasonable, shorter recovery time.

- Industry-wide LOOP nonrecovery curves are generally used for the analysis of a degraded condition where no LOOP event occurred or the analysis of an actual LOOP initiating event where event details are not initially well known. The latter case may be appropriate for a preliminary MD 8.3 evaluation. LOOP nonrecovery curves are based on actual operating experience where emergency power was available (i.e., conditions that do not represent SBO conditions).

Guidance for the use of these methods is discussed below.

- ***SPAR-H Method (Recovery Model).*** In an analysis of an actual LOOP event where the cause is well known, the SPAR-H method may be used for estimating probabilities of nonrecovery actions identified in LOOP and SBO sequences. Considerations for using the SPAR-H method in the recovery analysis include:
  - Key assumptions used to adjust the values of performance shaping factors (PSFs) should be confirmed by inspections.
  - Recovery actions should be supported by actions required in procedures, analysis, and operator training plans. Refer to the Section 6 for additional details.
  - Complications observed during recovery of offsite power.
  - Complexities of the recovery actions, while considering the context in which each operator action occurs; wherein this context is invariably sequence and cut set specific.
  - A task analysis should be performed to identify the steps needed to restore power to the first vital bus, given the accident sequence of interest. The recovery path may be different during SBO conditions than the path actually taken during the event.

[47] The mission time for a LOOP event analysis is typically 24 hours. However, an analysis of the shutdown risk of an extended LOOP event for greater than 24 hours may be warranted.

- For an easy identifiable electrical fault that causes a LOOP event, an assumption of 30 minutes may be appropriate to use as the time needed to restore power from an available power source, around the fault (if necessary), to first vital bus. These faults are usually self-revealing (e.g., lighting strike, maintenance-induced breaker action) and easily bypassed with minimal breaker operations.
- A detailed task analysis may support a recovery time of less than 30 minutes. However, when there are observed complications, a detailed task analysis may justify a longer recovery time. The feasibility of a 30-minute recovery time should be confirmed.

- ***Industry-Wide LOOP Nonrecovery Curves (Recovery Model).*** The probabilities of nonrecovery of offsite power to the first safety bus for various recovery times are provided in Table 4-1 in NUREG/CR-6890, "Reevaluation of Station Blackout Risk at Nuclear Power Plants." The data from Table 4-1 in NUREG/CR-6890 was used to generate LOOP nonrecovery curve parameters for the SPAR models. Considerations for using the curves in the recovery analysis include:
  - Industry-wide LOOP nonrecovery curves are generally used in a preliminary analysis of an actual LOOP event where event details are not initially well known.
  - The top part of Table 4-1 in NUREG/CR-6890 provides nonrecovery probabilities by LOOP duration and LOOP classes listed under the "LOOP Category" heading. The selection of the LOOP class should be based on the source of the fault or failure. The LOOP classes from NUREG/CR-6890 include: plant-centered, switchyard-centered, grid-related, and severe-weather-related. The table below provides the definitions of the different LOOP classes described in NUREG/CR-6890.

LOOP Class	Definition
Plant-Centered	*A LOOP event in which the design and operational characteristics of the nuclear power plant unit itself play the major role in the cause and duration of the loss of offsite power.* Plant-centered failures typically involve hardware failures, design deficiencies, human errors, and localized weather-induced faults (e.g., caused by lightning). The line of demarcation between plant-centered and switchyard-centered events is the nuclear power plant main and station power transformers high-voltage terminals. Both transformers are considered part of the switchyard.
Switchyard-Centered	*A LOOP event in which the equipment or human-induced failures of equipment in the switchyard play the major role in the loss of offsite power.* The line of demarcation between switchyard-centered events and grid-related events is the output bus bar in the switchyard. The bus bar is considered part of the switchyard.
Grid-Related	*A LOOP event in which the initial failure occurs in the interconnected transmission grid that is outside the direct control of plant personnel.* Failures that involve transmission lines from the site switchyard are usually classified as switchyard-centered events if plant personnel can take actions to restore power when the fault is cleared. However, the event should be classified as grid related if the transmission lines fail from voltage or frequency instabilities, overload, or other causes that require restoration efforts or corrective action by the transmission operator.

LOOP Class	Definition
Severe-Weather-Related	*A LOOP event caused by severe or extreme weather, in which the weather was widespread, not just centered on the site, and capable of major disruption. Severe weather is defined to be weather with forceful and non-localized effects.* An example is storm damage to transmission lines instead of just debris blown into a transformer. This does not mean that the event had to actually result in widespread damage, as long as the potential is there. Examples of severe weather include thunderstorms, snow, and ice storms. Lightning strikes, though forceful, are normally localized to one unit, and so are coded as plant centered or switchyard centered. Hurricanes, strong winds greater than 125 miles per hour, and tornadoes are examples of extreme-weather-related LOOPs.

  - The event and condition assessment (ECA) workspace in Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) provides the option to select one of four LOOP initiating event classes (plant-centered, switchyard-centered, grid-related, and severe-weather-related) based on LOOP classifications and frequency-weighted average recovery failure probabilities from NUREG/CR-6890. The ECA workspace will calculate probabilities for each LOOP nonrecovery basic event (e.g., OEP-XHE-XL-NR01H, -NR02H, -NR03H) given the LOOP class selected. LOOP nonrecovery basic event parameters should be set to TRUE for those parameters with recovery times less than the actual recovery time observed in the actual event.[48]
  - A thorough recovery analysis should be performed using the SPAR-H method recovery model once detailed information about the event is known.

- ***LOOP Nonrecovery Parameter Adjustments in SPAR Models.*** SPAR models have LOOP nonrecovery events for various recovery time increments. For example, OEP-XHE-XL-NR01H represents the nonrecovery event for 1-hour sequences. All SPAR models contain the generic set of nonrecovery parameters, but only a selection of parameters are used in a plant-specific model. Check that a LOOP nonrecovery parameter is not used before omitting an adjustment. Selection of any LOOP class in ECA will automatically modify all the LOOP nonrecovery basic events that are in the SPAR model. Review of the sequence cut-sets will allow the analyst to identify which basic events are used. If necessary, the probabilities for nonrecovery events based on the selected recovery model chosen can then be entered in the ECA analysis.

- ***Switchyard Boundary.*** Recognizing the physical boundary of a plant switchyard varies from plant-to-plant, it is generally assumed that the boundary for a LOOP event analysis starts at the first feeder breaker from the grid, which is controlled by the plant owner. In addition, the boundary for LOOP event analysis should also include any station auxiliary transformer(s) and/or shutdown transformers. Some plant owners may not own the switchyard and have to rely on the utility or transmission/distribution operator to restore power to the switchyard. Considerations for modeling the LOOP event at a switchyard include:
  - *Treating the switchyard as part of the grid.* If power had to be recovered from outside the owner controlled property, then the actual time that the control room was informed of

[48] For example, if the actual recovery time was two hours, then set OEP-XHE-XL-NR01H to TRUE. Leave the remaining nonrecovery parameters with nominal default values associated with the LOOP class.

available power in the switchyard may be appropriate when estimating the *Time Available* PSF level in SPAR-H method.

- *Confirmation by the inspection team on power stability from the offsite power source.* Once power from the offsite power source or grid was judged and observed to be stable (voltage and frequency) enough to carry critical loads associated with sequences of interest, a zero probability of another LOOP within a 24-hour period following recovery may be assumed in the analysis.
- *Documentation.* Define the grid/plant boundary in the analysis report. The term "grid" is often defined differently.

- ***Double Crediting Recovery Actions.*** Avoid crediting an alternate power source (black-start, cross-tie) given recovery of offsite power within a short period of time. Check for double crediting of nonrecovery terms in the minimal cut sets after model solution.

- ***Recovery Following Battery Depletion.*** The following recovery actions are not normally credited following battery depletion to avoid underestimating risk:
  - Offsite power recovery due to the manual closing of large, high-energy breakers.[49]
  - Local control of a turbine-driven pump using local steam generator level indications.
  - EDG recovery unless the EDG has its own DC power supply for start and control, and no loss of EDG cooling.

- ***SRV/PORV Demands*.** Adjust the failure probability for a safety relief valve (SRV) or power-operated relief valve (PORV) to close in the LOOP model to reflect the total number of primary SRV or pressurizer PORV demands that were observed during the transient. A binomial expansion of the nominal failure probability based on the number of demands is an acceptable approach.

- ***PRA Mission Time Adjustments.*** Mission time for key components with high fail-to-run probabilities can be based on the actual event timeline. Considerations include:
  - *EDGs.* The mission time variable in the EDGs fail-to-run probability should be based on the actual time that offsite power was restored to the first safety bus. This assumes that (1) actual event timeline are factored into the analysis, (2) EDGs are typically secured shortly following offsite power recovery, except for periods of grid instability, and (3) core damage would not occur given the availability of one train of safety systems powered from offsite power.
  - *Turbine-driven auxiliary feedwater (AFW) pump.* The mission time variable in the turbine-driven AFW pump fail-to-run probability should be based on the actual time that offsite power was restored to the second safety bus providing power to motor-driven AFW pumps. This assumes that (1) actual event timeline are factored into the analysis and (2) the risk contribution of a turbine-driven AFW pump failure to run following the recovery of offsite power to all motor-driven pumps is low.
  - A sensitivity analysis to show the importance of a mission time adjustment for each of these components.

[49] Switchyard breakers may have separate battery supplies. Typically, in-plant 7 kilo-volt (kV) and 4 kV breakers rely on station battery supplies.

- ***BOP Availability.*** For a total LOOP event with BOP loads powered from offsite power source, consider the following:
  - *Main feedwater (MFW) and condenser heat sink*. Availability and recovery of MFW and condenser heat sink:
    - If a reactor trip occurred and the LOOP did not affect offsite power supply to MFW and/or condenser heat sink loads, then consider the use of the loss of feedwater or transient event tree model. This generally works well for short-term LOOPs where nonrecovery of power, battery depletion, and related SBO issues do not significantly affect the risk analysis. For longer term LOOPs, consider adding MFW and/or condenser heat sink into the LOOP and SBO models.
    - Use the SPAR-H method to estimate the nonrecovery probability of MFW and/or condenser heat sink.
    - For boiling-water reactors (BWRs), the condenser heat sink may be available throughout the event. However, for short term sequences, recovery of condenser vacuum, if initially lost after the scram, may not be feasible.
  - *SRV/PORV demand parameter reduction.* If the condenser heat sink was not affected, then the probability of SRV or PORV challenges may be less likely. If there were no observed demands during the actual event, consider using the demand probability used for general transient events.
  - *Reactor Coolant Pump (RCP) seal cooling [only in pressurized-water reactors (PWRs)].* Normal RCP thermal barrier cooling may be powered from an energized non-safety-related electrical bus. Note: In most plants, thermal barrier cooling is from Component Cooling Water (CCW) pumps aligned to safety buses. In Westinghouse plant designs, seal injection via charging is powered from a safety bus, but may not be sequenced on a LOOP/SI signal. For most plants (except Prairie Island), CCW cools the charging pumps.
  - *Instrument air.* Station instrument air and associated systems supported by instrument air system may not be affected or may be readily recoverable.
  - *Other systems.* Check cut sets for other systems that may not apply given availability of BOP systems that remain functional

- ***RCP Seal Performance Issues (only in PWRs)***. Review RCP seal performance issues that were observed during the event.
  - If there were no indications of anomalous RCP seal performance, but actual plant conditions may have precluded timely operator actions, consideration should be given to the adjustment of human error probability parameters in the SPAR model RCP seal cooling event tree. Operator actions that are modeled in the SPAR model include:
    - OPR-XHE-XM-RSSDEP: Operator fails to rapidly depressurize primary pressure less than 1710 psi within 2 hours (*Westinghouse model*).
    - RCS-XHE-XM-CBOFF: Operator fails to isolate RCP seal controlled bleed off (*Combustion Engineering model*).
    - RCS-XHE-XM-SUBCOOL: Operator fails to maintain RCS sub-cooling greater than 50ºF (*Combustion Engineering model*).
    - RCP-XHE-XM-TRIP: Operator fails to trip reactor coolant pumps (*Westinghouse and*

Combustion Engineering models).[50]

- If there were some indications of an extended loss of or failure to restore RCP seal cooling in a timely manner, consider adjusting the default RCP seal failure probabilities. In addition, adjustments should be made if an actual failure of one or more stages of RCP seals were observed during the actual event.
- Refer to the RCP Seal Loss-of-Coolant Accident (LOCA) Model section in the plant SPAR model manual for details.

- ***Other Modeling Considerations.*** Other considerations include:
  - *Event and plant conditions at the time of the event.* Refer to Table 10-1, Part 1, “Initial plant configuration,” and Part 2, “Event description,” for additional items to consider in the analysis.
  - *As-built, as-operated plant.* Refer to Table 10-1, Part 5, “As-built, as-operated LOOP-related plant features,” for items to consider in the SPAR model.
  - *Plant-specific failure probabilities.* Plant-specific failure probabilities of key components may be higher or lower than the average industry estimates used in SPAR model parameter estimations. Key LOOP and SBO components include emergency diesel generator, turbine-driven pumps, and SBO/black-start power source.
  - *LOOP analysis model in SPAR models.* Refer to the “Loss of Offsite Power Model” section in the plant-specific SPAR model manual for details about calculation of LOOP frequencies, LOOP nonrecovery probabilities, and EDG nonrecovery probabilities.

10.5 Risk Quantification

The risk quantification of a LOOP event is similar to the analysis of other initiating events, as described in Appendix A. Specific considerations for the analysis of LOOP events include:

- As for any initiating event analysis, the LOOP initiator is set to 1.0, because it happened.

- The method most frequently used in many PRA models for addressing timing issues is the use of convolved distribution models. Using this method, mathematical functions that describe the distribution of the diesel failure time data and the distribution of offsite power duration data are joined to create a new distribution that describes the probability of these cut sets.[51] Inclusion of this convolution credit can have a significant effect on reducing SBO core damage frequency estimates (in some cases, approaching an order of magnitude) for plants with two EDGs.

- Current versions of the SPAR models use the convolution method described above. The specifics are provided with the SPAR model documentation. Consult Idaho National Laboratory for any necessary modifications of this feature in an analysis.

[50] The SPAR model LOOP event tree assumes that all RCPs trip due to loss of offsite power.

[51] Effectively, the convolution calculation breaks up the time between 0 and 8 hours into small increments. In each increment, the probability of the EDG failing to run in that increment is calculated, and multiplied by the probability of offsite power not being recovered by the end of that increment. The product of the two parameters is taken because of the assumption that EDG recovery and offsite power recovery are statistically independent.

10.6 Uncertainty Considerations

Sources of uncertainties in analyzing risk of LOOP initiating events include the following:

- LOOP nonrecovery probability estimates based on the chosen recovery model and offsite power recovery time estimate.

- Reliability of the station blackout (or black-start) power source.

- Stability of the offsite power source following a grid disturbance or during extreme-weather conditions.

- Nonrecovery estimates of key component failures (e.g., EDGs, turbine-driven AFW pumps) that were observed during the actual event.

- Modeling operator performance deficiencies that were observed during the actual event.

Table 10-1. Information typically needed for the risk analysis of LOOP initiating events.

1. ***Initial plant configuration–*** Plant configuration prior to the initiating event *(Note: In some plant electrical distribution systems, attention should be paid to a dedicated sequencer panel with load shed relays and their system interactions)*:

☐ Equipment out-of-service for test or maintenance

☐ Electrical power lineups (note any unusual lineups due to ongoing maintenance or surveillance testing)

☐ Reactor coolant pump seal type (PWRs)

☐ Pressurizer PORV block valves open/closed during power operation (PWRs)

☐ Power history (time of last plant shutdown)

2. ***Event description–*** Elements of event timeline:

☐ Fault that caused LOOP
- Location of fault(s)
- Cause of fault(s)

☐ Restoration of power to first owner-controlled switchyard breaker:
- Important actions taken by the plant and outside organizations to recover power
- Time when power from the grid stabilized
- Time when the control room was informed

☐ Status of alternate power sources, such as black-start equipment and crossties (see note 1):
- Equipment start and load
- Time when equipment was secured
- Observed problems (e.g., trips, reduced performance)

☐ Status of emergency power sources (e.g., diesel generators):
- Equipment start and load
- Time when equipment was secured
- Observed problems (e.g., trips, reduced performance)

☐ Depletion of plant and switchyard batteries, if any

☐ Status of safety systems (e.g., AFW, high-pressure injection):
- Automatic actuations
- Manual actuations
- Time when equipment was secured
- Observed problems (e.g., trips, reduced performance)

☐ Status of BOP systems:
- Power lost and recovered to non-safety-related BOP buses
- Availability of main feedwater and primary conversion system
- Loss of condenser hear sink
- Main steam isolation valve isolations
- Loss of main feedwater pumps
- Loss of instrument air

☐ Primary safety relief valve(s) and/or PORVs (PWR) demands (include each demand, if possible)

☐ Equipment failures and performance issues observed during the event:
- Switchyard

- o In-plant electrical distribution system
- o Safety systems
- o BOP systems
- o Reactor coolant pump seals (PWR)

☐ Failed or out-of-service equipment recovered during event

☐ Recovery of offsite power to each vital bus

☐ Operator performance issues

3. ***Offsite power recovery–*** Detailed information about offsite power recovery actions observed during the actual event:

☐ Availability of offsite power to carry electrical loads to mitigate reactor coolant pump seal (PWR) or stuck open safety/relief vale LOCA and to bring the plant to cold shutdown:
- o Actual time when offsite power was stable (voltage and frequency)
- o How was this time determined?
- o Estimated time when control room staff knew that offsite power was stable to carry critical electrical loads

☐ Delineation of owner controlled breakers in the switchyard and black-start capability (most can be found in plant procedures):
- ○ Plant control boundary
- ○ Breaker controls and start capability in the control room
- ○ Communications needed with outside organizations including another control room of a multi-unit site
- ○ Availability of outside organizations 24/7

☐ Steps taken to recover offsite power to the first safety bus including control room and local actions

☐ Breaker alignments
- o Actual path taken to bring in offsite power to safety buses
- o Alternative success paths to bypass the electrical fault

☐ Estimate of the earliest time when offsite power could have been restored to the first safety bus given a postulated station blackout or other EDG failure sequence, such as the loss of one bus and the failure of a key component powered from the remaining bus.

☐ Operator and equipment performance issues

4. ***Equipment initiation and recovery–*** Assessment of the actuation or recovery of risk-important systems as determined by preliminary SPAR model analysis:[52]

☐ Typical systems that are important to risk contribution during LOOP and station blackout sequences are as follows:
- ○ Recovery of offsite power to the first safety bus (refer to Item 3)
- ○ Start and load of alternate power sources
- ○ Recovery of failed equipment
- ○ Recovery of equipment in test or maintenance
- ○ Recovery of MFW (turbine- or motor-driven pump)
- ○ Recovery of condenser heat sink
- ○ Recovery of instrument air

[52] This information will be used in the HRA to estimate the performance shaping factor levels for time available, complexity, and procedures. Other considerations (e.g., stress, experience/training, ergonomics, fitness for duty, work processes) will be included in the HRA by the analyst to estimate a nonrecovery probability.

- ☐ Assessments should be performed in the context of the applicable core damage sequence, even if the system was not initiated or recovered during the actual LOOP event. Each assessment should include
  - ○ Determination whether the recovery is creditable within the component PRA mission time (usually 24 hours) given the nature of the equipment damage.
  - ○ List of operator actions, including diagnostic actions and repair/recovery actions inside and outside the control room.
  - ○ Time needed to complete the action, including upper and lower bounds. In some cases, the actual time observed during the event may be a reasonable approximation for the mean/average time, excluding the time taken for paper work.
  - ○ Availability of necessary information for worst case scenarios:
    - ▪ Procedures
    - ▪ Plant staffing with the necessary skills
    - ▪ Staffing of key external support organizations (e.g., transmission dispatch operators)
    - ▪ Tools
    - ▪ Lighting; electrical power for tools
    - ▪ Spare parts

5. ***As-built, as-operated LOOP-related plant features–*** Information used during the review of the SPAR model to ensure that the model reflects LOOP-related as-built, as-operated plant features:

- ☐ Alternate AC power sources (black-start, portable generators) and reliability issues (see Note 1)

- ☐ Improvements in reliability of black-start capability, such as replacements or upgrades (see Note 1)

- ☐ Cross ties between plants (refer to item 6, below, for criteria for crediting cross ties):
  - ○ Shared emergency diesel generator
  - ○ Cross-tie of the Division III (high-pressure core spray) bus to another bus (BWR 5/6)
  - ○ Transformer
  - ○ Bus cross connect
  - ○ Auxiliary feedwater pump (PWR)
  - ○ Others (specify)

- ☐ Rated battery depletion times:
  - ○ Station batteries
  - ○ Switchyard batteries
  - ○ Diesel generator batteries
  - ○ Implemented load shedding or extended battery depletion times

- ☐ Reactor coolant pump seal design (PWR)
  - ○ Seal design type
  - ○ Seal cooling systems
  - ○ Coping time without seal cooling

- ☐ Diesel-driven pump(s)

- ☐ Fire protection water pump(s)

- ☐ Pressurizer PORV block valves normally closed during power operation (PWR)

6. ***Alternative mitigating strategy–*** Documentation that supports the use of a unique plant design or operating feature. The bases for crediting a mitigating strategy or system include:

- ☐ *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.

☐ *Confirmatory inspections* to verify feasibility of alternative strategy.

7. ***Procedures–*** Relevant emergency, abnormal, and special operating procedures, which were in effect at the time of the event:

☐ Reactor trip and post trip

☐ LOOP event

☐ Station blackout

☐ Recovery of power to the switchyard with and without DC power

☐ Recovery of power to the safety buses

☐ Battery life extension (load shedding)

☐ Operation of alternate power sources, including black-start sources (see Note 1)

8. ***Plant drawings–*** Electrical distribution drawings showing:

☐ Switchyard

☐ Safety buses and loads

☐ BOP buses and loads

Note:

1. Black-start capability refers to any on-site power source that is capable of re-powering one or more vital AC buses under SBO conditions. Availability of a black-start power source is typically modeled in the plant's PRA model, even if the black-start source is controlled, operated, and maintained by an outside organization. However, the use must be proceduralized and staff readily available to start the alternate power source. If black-start capability was not credited in the plant PRA, then administrative controls must be carefully looked at for the appropriate credit in the SPAR model. Considerations include human error probabilities for fail-to-start (FTS) and load first vital bus, and nominal probabilities for FTS, fail-to-run, and test and maintenance.

11. Support Systems Initiating Events

11.1 Objective and Scope

The objective of this guide is to address the use of the new fault tree modeling of Support Systems Initiating Events (SSIEs) within the standardized plant analysis risk (SPAR) models for Significance Determination Process (SDP), Accident Sequence Precursor (ASP), or Management Directive (MD) 8.3, "NRC Incident Investigation Program," assessments.

11.2 Background

SSIEs are defined in Electric Power Research Institute (EPRI) Technical Report 1016741, "Support System Initiating Event, Identification and Quantification Guideline," as: "Any event such as a component, train, or complete system failure (or causing the failure of a component, train, or system) that:

- Challenges a reactor safety function, then
- Leads to a reactor trip, and also
- Fails a train or complete front-line system normally available to respond to the reactor trip or reactor shutdown and successfully mitigate the loss of the critical safety function."

This definition not only requires the failure to cause a reactor trip, but the failure must also reduce the mitigation capabilities of the engineered safety systems to prevent core damage. However, event and condition assessments (ECAs) will not be analyzing SSIEs (by definition) in most cases, but rather the failure or unavailability of support system structures, systems, or components (SSCs) which increases the SSIE frequency and failure probability of mitigation function of the applicable support system.

The NRC has decided to incorporate SSIEs for the fluid and air systems in the SPAR models in order to align with best practices and to meet requirements of the American Society of Mechanical Engineers (ASME) PRA Standard.[53] Pressurized-water reactor SPAR models include loss of service water (SW), loss of component cooling water (CCW), and loss of instrument air (IA) initiating event fault trees. Boiling-water reactor SPAR models will include loss of SW, loss of reactor/turbine building closed-loop cooling water, and loss of IA initiating event fault trees.[54]

From the three methods proposed for modeling SSIEs in in EPRI Technical Report 1016741, the NRC has chosen to employ the explicit event methodology (i.e., carry the fault tree logic cut sets through the event tree) in the SPAR models.[55] This decision was made in part because of

[53] The PRA Standard referred in this handbook includes ASME RA-Sa-2009, as endorsed by Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities."

[54] Support system initiating events that contribute less than one-percent of the total plant core damage frequency have been excluded from SPAR models.

[55] The other two methodologies are the point estimate fault tree methodology and the multiplier methodology.

the method's ability to illustrate the basic event contribution to the initiating event total frequency and allow the same components to be failed when analyzing the other event trees (e.g., transient). In addition, the impact of the individual components can be viewed in the cut sets and importance measures.

11.3 Explicit Event Methodology

- ***Brief Description.*** The explicit event methodology uses both initiating events and enabling events to represent each component or train within a support system. Both representations are needed for each component or train since a failure of a support system usually requires multiple components to fail simultaneously or within a brief period. Therefore, the initiating event causes the loss of the support system if and only if the appropriate enabling events (i.e., additional component failures) are present. Initiating events are quantified as the frequency at which each component or train fails in a year. The enabling events represent the component's unavailability, or the probability the component will fail or be in a failed state at the time of an initiating event.

- ***Method Options.*** The explicit method can be used in two different ways. The first option is to isolate the initiating event model in a fault tree and then only use it to provide the initiating event frequency of the support system. The second option is to allow the initiating event model cut sets to be carried through the event tree logic and appear in the sequence cut sets. Both options are similar in modeling and therefore have similar advantages and disadvantages. The major difference between these two options is that the second option allows the individual components to be carried through the sequence cut set generation and calculation.

11.4 SPAR Model Manipulations for ECA

- ***Activating SSIE Logic***. The SSIE logic is currently turned off in the applicable SPAR models.[56] Once the SSIE logic has been incorporated into all of the SPAR models, the logic will be activated in all the base models. In the meantime, the analyst can activate the logic (if needed) to support an analysis using the following steps:
  - Select the applicable initiating event (e.g., IE-LOCCW, IE-LOSWS, and IE-LOIA), set the *Default Template* box to NOT ASSIGNED, unselect the *Frequency* box and set the Frequency to 1.0.
  - Select the *Process Flag* for the corresponding SSIE fault tree (e.g., IEFT-LOCCW, IEFT-LOSWS, IEFT-LOIA) to FAILURE=> SYSTEM LOGIC | SUCCESS=> DELETE TERM.
  - Resolve the model by selecting all of the event trees, right click and select SOLVE. Check the *Copy Cut Sets to Nominal Case* box and select SOLVE.

- ***ECA of Support System Component(s) Failure.*** To perform a condition analysis of a support system component(s) failure, the analyst should perform the following steps:
  - For a failure of component that has an associated initiating and enabling basic events (e.g., CCW heat exchangers, CCW and SW pump(s) failures to run, IA compressor(s) failures to run, SW strainers/traveling screens, and key SW valves):

[56] As of June 1, 2012, a total of 37 SPAR models have had the SSIE logic incorporated.

    - Select the enabling basic event for the applicable component and set the *Failure Model* to TRUE.
    - Select the corresponding component initiating event and set the *Failure Model* to FALSE.[57]
    - If the support system components were in a specific configuration for the entire exposure period, set the appropriate configuration basic events accordingly.

      Example– For the past 15 days, CCW Pumps A and C were running, with CCW Pump B in Standby. Pump A fails while running and Pump B successfully auto-starts and runs. It takes the licensee two days to repair the pump before testing is complete and the pump is declared operable. The exposure period of is approximately two days. The analyst would set the CCW-MDP-FR-A to TRUE and IE-CCW-MDP-FR-A to FALSE.[58] In addition, since the exposure time essentially starts with Pump A unavailable, and Pumps B and C running, the analyst would set the configuration event for *CCW Pumps B and C Running, Pump A in Standby* to TRUE, and set the other configuration events to FALSE.

  - For a failure of components that only has an associated enabling event (e.g., CCW and SW pump failures to start and CCW, SW, and IA component without associated initiating basic events):
    - Select the enabling basic event for the applicable component and set the *Failure Model* to TRUE.
    - If the support system components were in a specific configuration for the entire exposure period, set the appropriate configuration basic events accordingly.

      Example– For the past 30 days, CCW Pumps A and C were running, with CCW Pump B in Standby. While preparing to switch running pumps, operators manually start CCW Pump B; however, the pump fails to start. Inspectors determine that pump had been inoperable since it was last run (30 days ago). It takes the licensee two days to repair the pump before testing is complete and the pump is declared operable. The exposure period is determined to be approximately 32 days. The analyst would set the CCW-MDP-FS-B to TRUE. In addition, Pumps A and C were running, with Pump B is standby during the entire exposure time. Therefore, the analyst would set the configuration event for *CCW Pumps A and C Running, Pump B in Standby* to TRUE, and set the other configuration events to FALSE.

11.5 Remaining Technical Issues

- Some CCF modeling techniques have not been fully developed, reviewed, and/or accepted by the staff/PRA community. These issues include (not an exhaustive list): using the new SAPHIRE CCF methodology for SSIE models, the conditional treatment of CCFs in the SSIE fault tree, and any additional issues identified during the initial use of the SSIE models.

- The accuracy of the cut set-based results can vary depending on the SSIE model repair assumptions. In addition, the cut sets may not capture the significant transient behavior of SSIE frequencies for time periods that may encountered in an ECA.

[57] For some SSCs, such as the CCW heat exchangers and SW strainers/traveling screens, two initiating basic events for the applicable SSC are in the applicable SSIE fault tree. One event is the initiating basic event associated with the failure of the applicable SSC due to electro-mechanical failures, while the other initiating basic event is associated with the failure of the applicable SSC due to an extreme environmental event (e.g., flora, fauna, debris, or ice). The initiating basic events associated with extreme environmental events should not be manipulated in an ECA for a failed component due to such events. Consult Idaho National Laboratory if an ECA potentially requires an adjustment of the extreme environmental initiating event basic event(s).

[58] The corresponding initiating event basic event is set to FALSE because a loss of CCW initiating event did not occur.

- The importance measures associated with the SSIE models calculated within the ECA module in SAPHIRE can be in error due to the explicit method calculation and depending on the analysis assumptions.

12. References

1. U.S. Nuclear Regulatory Commission, Management Directive 8.3, “NRC Incident Investigation Program,” June 2014 (ADAMS Accessions No. ML13175A294).

2. U.S. Nuclear Regulatory Commission, Inspection Manual Chapter 0609, “Significance Determination Process,” April 2015 (ADAMS Accession No. ML14153A633)

3. U.S. Nuclear Regulatory Commission, Inspection Manual Chapter 0308, “Reactor Oversight Process Basis Document,” September 2014 (ADAMS Accession No. ML14164A209).

4. U.S. Nuclear Regulatory Commission, Inspection Manual Chapter 0309, “Reactive Inspection Decision Basis for Reactors,” October 2011 (ADAMS Accession No. ML111801157).

5. U.S. Nuclear Regulatory Commission, “Risk Assessment of Operation Events Handbook—External Events,” Volume 2, Revision 1.01, January 2008 (ADAMS Accession No. ML080300179).

6. U.S. Nuclear Regulatory Commission, “SPAR Model Reviews,” Volume 3, Revision 2, September 2010 (ADAMS Accession No. ML102850267).

7. U.S. NRC, “PRA Review Manual,” NUREG/CR-3485, September 1985.

8. American Society of Mechanical Engineers, “Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,” RA-Sa-2009, February 2009.

9. 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 2, March 2009 (ADAMS Accession No. ML090410014).

10. U.S. Nuclear Regulatory Commission, “Shutdown Events,” Volume 4, Revision 1, April 2011 (ADAMS Accession No. ML111370163).

11. U.S. Nuclear Regulatory Commission, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” NUREG/CR-6823, September 2003 (ADAMS Accession No. ML032900131).

12. U.S. Nuclear Regulatory Commission, “Good Practices for Implementing Human Reliability Analysis (HRA),” NUREG-1792, April 2005 (ADAMS Accession No. ML051160213).

13. U.S. Nuclear Regulatory Commission, “Evaluation of Human Reliability Analysis Methods against Good Practices,” NUREG-1842, September 2006 (ADAMS Accession No. ML063200058).

14. U.S. Nuclear Regulatory Commission, "SPAR-H Human Reliability Analysis Method," NUREG/CR-6883, August 2005.

15. U.S. Nuclear Regulatory Commission, "Technical Basis and Implementation Guide for a Technique for Human Event Analysis," NUREG-1624, May 2000 (ADAMS Accession No. ML003719212).

16. U.S. Nuclear Regulatory Commission, "ATHEANA User's Guide," NUREG-1880, June 2007 (ADAMS Accession No. ML072130359).

17. U.S. Nuclear Regulatory Commission, "EPRI/NRC RES Fire PRA Methodology for Nuclear Power Facilities," NUREG/CR-6850, Volumes 1 and 2 (including Errata and Supplement 1, September 2005.

18. U.S. Nuclear Regulatory Commission, "Handbook for Phase 3 Fire Protection Significance Determination Process Analysis," December 2005 (ADAMS Accession No. ML053620267).

19. U.S. Nuclear Regulatory Commission, "Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 8," NUREG/CR-7039, Volumes 1–7, June 2011.

20. Idaho National Laboratory, "SPAR-H Step-by-Step Guidance," INL/EXT-10-18533," May 2011.

21. U.S. Nuclear Regulatory Commission, "A Review of NRC Staff Uses of PRA," NUREG-1489, June 2007, (ADAMS Accession No. ML063540593).

22. U.S. Nuclear Regulatory Commission, "Reevaluation of Station Blackout Risk at Nuclear Power Plants," NUREG/CR-6890, Volumes 1–3, December 2005.

23. 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 (ADAMS Accession No. ML070650650).

24. U.S. Nuclear Regulatory Commission, "Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding," NURE/CR-6268, September 2007 (ADAMS Accession No. ML072970404).

25. U.S. Nuclear Regulatory Commission, "NRC Staff Position on Crediting Mitigating Strategies Implemented in Response to Security Orders in Risk-Informed Licensing Actions and in the Significance Determination Process," Regulatory Information Summary 2008-15, June 2008 (ADAMS Accession No. ML080630025).

26. Nuclear Energy Institute, "Qualitative Assessment for Crediting Portable Equipment in Risk-Informed Decision Making," December 2015 (ADAMS Accession No. ML16138A018).

27. Nuclear Energy Institute, "Streamlined Approach for Crediting Portable Equipment in Risk-Informed Decision Making," December 2015 (ADAMS Accession No. ML16138A017).

28. U.S. Nuclear Regulatory Commission, Memorandum from W. Dean (NRC) to A. Pietrangelo (NEI), August 9, 2016 (ADAMS Accession No. ML16167A034).

29. Nuclear Energy Institute, "Crediting Mitigating Strategies in Risk-Informed Decision Making" NEI-16-06, August 2016 (ADAMS Accession No. ML16286A297).

30. U.S. Nuclear Regulatory Commission, "Assessment of the Nuclear Energy Institute 16-06, 'Crediting Mitigating Strategies In Risk-Informed Decision Making,' Guidance For Risk-Informed Changes To Plants Licensing Basis," Memorandum form M. Reisi-Fard to J. Giitter, May 30, 2017 (ADAMS Accession No. ML17031A269).

31. Electric Power Research Institute, "Establishing Minimum Acceptable Values for Probabilities of Human Failure Events: Practical Guidance for PRA," EPRI Technical Report 1021081, October 2010.

32. U.S. Nuclear Regulatory Commission "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," NUREG-1278, August 1983 (ADAMS Accession No. ML071210299).

33. Electric Power Research Institute, "Support System Initiating Event, Identification and Quantification Guideline," EPRI Technical Report 1016741, December 2008.

This page intentionally left blank.

Appendix A– Road Map for Risk Analysis of Operational Events

Introduction

The following road map describes generic methods and processes to estimate the risk significance of initiating events [e.g., reactor trips, losses offsite power (LOOPs)] and degraded conditions [e.g., a failed high-pressure injection pump, failed emergency diesel generator (EDG)] that have occurred at nuclear power plants.

In this road map, “initiating event” and “degraded condition” are used to distinguish an incident involving a reactor trip demand from a loss of functionality during which no trip demand occurred. The overall term used to collectively refer to these analyses is event and condition assessments (ECA).

Overview

Process Overview. The overall event analysis process involves the modification of a standardized plant analysis risk (SPAR) model to reflect attributes of an event, solution of the modified model to estimate the risk significance of the event and documentation of the analysis and its results. The process is structured to ensure the analysis is comprehensive and traceable. A detailed review by the analyst and a subsequent independent review(s) minimize the likelihood of errors, and enhance the quality of the risk analysis.

As a minimum, a risk analysis consists of the following:

- Development of a risk-focused understanding of the event that occurred, relevant plant design, and operational features as well as the status of the plant.

- Comparison of the event with the existing risk model to identify any changes that are necessary to support the analysis.

- Risk model elaboration, if necessary, to allow the risk-related features of the observed event to be properly represented in the model.

- Model modification to reflect event specifics.

- Initial model solution to estimate the risk significance of the event without consideration of crew activities to recover risk-significant failures.

- Recovery analysis to address potential crew actions to recover any failed components associated with risk-significant sequences.

- Analyst review of the results to ensure that the logic model and incident mapping process is correct. The focus of this review is to identify inconsistencies, errors, and incompleteness in the SPAR model. Then the SPAR model is modified and re-solved.

- Final documentation of the inputs (facts), assumptions, results, and uncertainties.

- Independent review(s) of the completed analysis.

In addition, a supplemental effort that can improve analysis accuracy and confidence in the results should be performed for higher risk-significance or controversial events:

- Sensitivity and uncertainty analyses to gain additional understanding of the impact of analysis assumptions and data variability on analysis results.

The event analysis process is iterative. Review of the model for applicability may highlight the need for additional detail related to the event. Review of the initial analysis results (significant sequences and cut sets) frequently identifies the need for additional detail concerning the event, plant design, operational information, or the need for greater model fidelity.

Risk Analysis Overview. The Significance Determination Process (SDP), accident sequence precursor (ASP), and Management Directive (MD) 8.3, "NRC Incident Investigation Program") analyses are retrospective analyses of an operational event. In these analyses, a "Failure Memory Approach" is used to estimate the risk significance of degraded conditions and initiating events. In a "Failure Memory Approach", risk model elements (basic events) associated with observed failures and other off-normal situations are configured to be failed, while those associated with observed successes and unchallenged components are assumed capable of failing, typically with nominal probability.

A failure is defined in terms of the inability of a component (or operator action) to function in the context of a particular risk sequence and mission time.[59] A risk analysis is performed on the failures and off-normal situations observed during an initiating event or degraded condition(s) discovered during surveillance test, engineering evaluation or inspection. A degraded condition may represent a failed or unavailable structure, system, or component (SSC) that was unable to perform its mission upon demand or a degraded SSC with a higher probability of failure to complete its mission.

All other components in the risk model that were not impacted or challenged by the operational event are modeled with nominal (i.e., random) failure probabilities. An event involving a reactor trip is analyzed as an initiating event, although the non-initiator parts of an initiating event can be addressed in a supplemental degraded condition analysis. Postulated failures, such as the postulated failure of pump B instead of the observed failure of pump A because pump B's failure is of higher risk significance, are not assumed in the event analysis (except as a sensitivity analysis).

Analysis Types. The detailed risk analysis of an operational event considers the immediate impact of an initiating event and/or the potential impact of the equipment failure(s) or operator error(s) on the readiness of systems in the plant for mitigation of off-normal and accident conditions. Three types of risk analysis are common: condition analysis, initiating event analysis, and shutdown analysis.

[59] A component can be considered failed for some sequences and not failed for others in which the requirements for successful mitigation are more relaxed. Component functionality is often unrelated to inoperability as defined in a plant's technical specifications (TS). A component that has been declared inoperable based on TS may be functional (and therefore not failed) from a risk standpoint.

Condition analysis. If the event or failure had no immediate effect on plant operation (i.e., no initiating event occurred), then the analysis considers whether the plant would require the failed items for mitigation of potential core damage sequences should a postulated initiating event occur during the failure period.

In this analysis, nominal initiating event frequencies are used in the analysis. The failure probability of the degraded component will be adjusted based on the degradation period to reflect the degree in which the component will fail during the required mission time. In some cases, extensive engineering analysis or expert judgment is required to determine the degree of degradation of the component. Nominal failure probabilities of all other components are used in the analysis. The risk analysis uses a maximum period of unavailability of one year.

A condition analysis can include the unavailability of multiple components that were discovered at different times. In this special case, the time period in which the components were unavailable must overlap to some degree. The conditional probability of the increase in risk caused by the unavailable components is integrated over the worst case one-year time period.

Initiating event analysis. If the event or failure resulted in an automatic or manual reactor trip and occurred while the plant was at power, then the event is evaluated according to the likelihood that it and the ensuing plant response could lead to core damage.

In this analysis, the frequency of the observed initiating event will be set to 1.0 (because it happened). If any component of a mitigating system failed along with the initiating event, including operator errors, then the failure probability of the failed equipment will be set to TRUE as specified in specific program guidance. All other initiators in the risk model are set to zero.

If a failure or degradation of a component was observed during the event, the failure probability of the component will be adjusted to reflect the degree in which the component will fail during the required mission time, similar to a condition analysis. Nominal failure probabilities of all other components are used in the analysis. The treatment of failures and degraded conditions in an initiating event analysis differ between the SDP, ASP Program, and MD 8.3 assessments. Refer to Section 8 for additional details on initiating event analyses.

Shutdown analysis. If the event or failure was identified while the plant was not at power, then the event is first assessed to determine whether it could have impacted at-power operation. If the event could have impacted at-power operation, its impact is assessed. If the event could only occur at cold shutdown or refueling shutdown, then its impact on continued decay heat removal during shutdown is assessed. Guidance for performing a risk analysis of shutdown events is provided in Volume 4 of this handbook.

Roadmap Overview. The analysis task flow is illustrated in Figure A-1. Each task depicted in the figure is summarized in the following road map.

Sections 2–7 provide additional guidance that details acceptable methods and approaches that have been applied, reviewed, and approved in past SDP, ASP, and MD 8.3 analysis. The tasks in the following road map will refer to these method-specific guides.

Iterative Nature of Analyses. As shown in Figure A-1, the risk analysis of an operational event is an iterative process. Many tasks in the analysis process may require the analyst to repeat or consider pervious tasks several times throughout the analysis. This iterative approach will eventually result in the convergence of the probabilistic risk assessment (PRA) model that best represents the as-built, as-operated plant and the operational event.

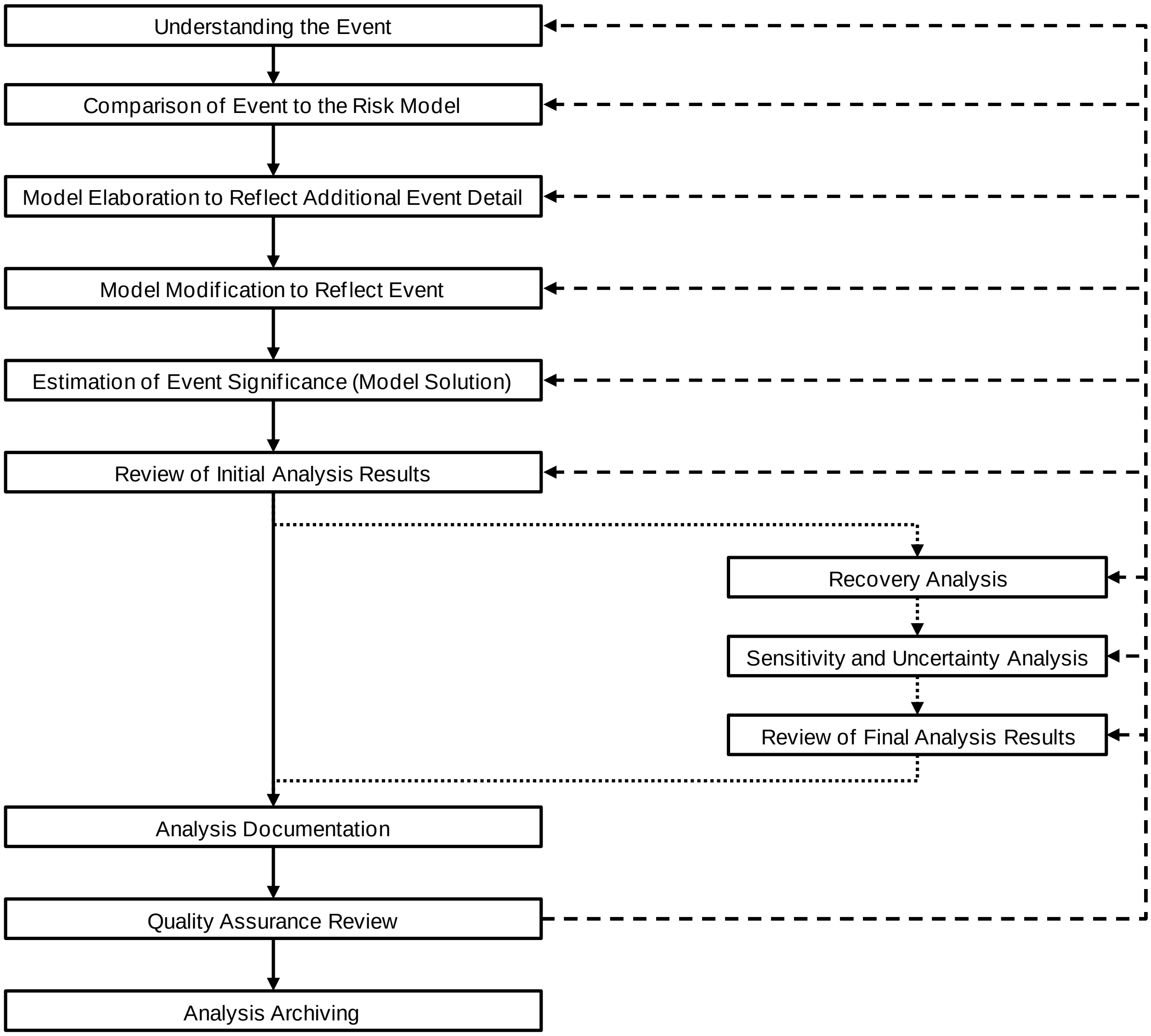

Understanding the Event
Comparison of Event to the Risk Model
Model Elaboration to Reflect Additional Event Detail
Model Modification to Reflect Event
Estimation of Event Significance (Model Solution)
Review of Initial Analysis Results
Recovery Analysis
Sensitivity and Uncertainty Analysis
Review of Final Analysis Results
Analysis Documentation
Quality Assurance Review
Analysis Archiving

Figure A-1. Risk Analysis of Operational Events—Process Flow.

Risk Analysis of Operational Events

□ **Step-1: Understanding the Event.** In the initial step in the analysis process, the analyst develops a comprehensive and detailed understanding of the event that occurred, including off-normal component and operator performance and unit and plant status. The event should be documented in sufficient depth to provide a reviewer or unfamiliar reader an in-depth understanding of risk-related issues associated with the occurrence.

Given the iterative nature of an analysis, some of these information collection activities may have to be readdressed in various steps throughout the analysis. Risk model solution and sensitivity analysis may be required prior to identification of risk important information.

- ***Step-1a: General Documentation Considerations.*** The event should be documented in sufficient depth to provide a reviewer or unfamiliar reader an in-depth understanding of risk-related issues associated with the occurrence. In addition, all factual information should refer to a traceable reference, such as root cause analyses, inspection reports, plant drawings, system descriptions, procedures, and discussions with agency and plant staff.

- ***Step-1b: Internal Event Information Considerations.*** For all situations, the description should include a time line that details the sequence of events. This time line is a chronology of all known occurrences observed during the event period of interest. The chronology also summarizes the analyst's understanding of relevant aspects of the event that can be reviewed by those familiar with the event for completeness and correctness. In addition, the chronology can be used as an outline to show the relationships between event occurrences, assumptions, uncertainties, and PRA model changes. Some considerations for initiating event analysis and condition analysis include the following:

  Information common to both initiating event and condition analyses include:

  - Unit and plant operating state(s) [including potential operating states that occurred around the time of the event (e.g., within two weeks) and could have further impacted the risk].
  - Components determined failed, degraded, and in test and maintenance (T/M). The sequence of events chronology should describe dates and times when equipment failed or was rendered unavailable and the dates and times when such equipment was restored to operability.
  - The status of support systems, in particular the configuration of systems with operating and standby trains.
  - Unavailability of other components discovered later, if appropriate for the analysis application. Refer to the program-specific procedure (i.e., SDP, ASP, and MD 8.3).
  - For completeness, the chronology should include occurrences not relevant to the risk analysis. The basis for such determination should be later included in the analysis documentation.

  Information applicable only to initiating event analyses includes:

  - Plant activities prior to the event initiator.
  - Observed initiating event initiator and reactor trip signal.
  - Systems demanded in response to the initiating event.
  - Systems/components discovered inoperable as a result of the initiating event.
  - Components that were not demanded during the event and were later (weeks or months) discovered unavailable during the event period.
  - Unexpected or spurious component actuation.
  - Operator actions performed in response to an initiating event (proceduralized and

non-proceduralized).

  - Operator actions to restore the functionality of a failed or unavailable component.
  - Operator actions that should have been performed during the response.
  - Other operator performance issues (e.g., slow response, observed higher than normal stress, unclear procedures, ergonomic issues, observed poor work processes).

  Information applicable only to condition analyses includes:

  - Relevant maintenance and testing history associated with the failed or degraded SSC.
  - Overlapping unavailability of other components, if appropriate for the analysis application. Refer to the program-specific procedure (i.e., SDP, ASP, and MD 8.3). Licensee event reports (LERs) issued at least one year before the first condition should be reviewed for other overlapping unavailable components.

- ○ ***Step-1c: External Events Information Considerations.*** Information useful for the analysis of external events in condition analysis and initiating event analysis is provided in Volume 2 of this handbook. Refer to the sections on modeling considerations for the following operational events:

  - Internal fire events,
  - Internal flooding events,
  - Seismic events, and
  - Severe-weather events.

- ○ ***Step-1d: LOOP Information Considerations.*** Information useful for the analysis of a LOOP initiating event is provided in Section 10.

□ **Step-2: Base Case SPAR Model Comparison with the Event and As-Built, As-Operated Plant.** Once an event is understood, the appropriateness of the existing SPAR model in describing the potential risk impact is confirmed. This analysis includes ensuring that the base case SPAR model reflects the as-built, as-operated plant for the sequences impacted by the operational event. Areas where additional modeling detail is required to adequately reflect the observed event are identified. Some considerations include the following:

- ○ Review the plant SPAR model manual to develop an understanding of the assumptions and details associated with the sequences and fault trees related to the event.

- ○ Confirm that the observed component impacts can be addressed in the model by setting basic events to TRUE or through probability modification. Review all basic events associated with an impacted component for applicability.

- ○ Refer to Section 2.1 of Volume 3 of this handbook for a review checklist covering the following considerations:

  - 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.

- ○ Refer to Section 2.2 of Volume 3 of this handbook for a review checklist covering the following considerations:
  - – To check whether the key assumptions in a SPAR model are adequately considered in the logic model for those 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.

- ○ Report SPAR model issues and suggestions for enhancements to the SPAR model developers at the Idaho National Laboratory. Use the feedback form from the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) User Group Web Page.

□ **Step-3: Base Case SPAR Model Elaboration to Reflect Additional Event-Related Detail.** Based on the information developed in the previous step, the base case SPAR model is modified as necessary to reflect the risk-related features of the event.[60] This step may include the following activities:

- ○ Review SPAR model assumptions
- ○ Event tree modification(s)
- ○ Fault tree modification(s)
- ○ Initiating event frequency parameter update(s)
- ○ Basic event parameter update(s)—component failure probability or rate
- ○ Basic event parameter update(s)—common-cause failure (CCF) probability
- ○ Basic event parameter update(s)—human error probability
- ○ Solving and saving the modified model

Some considerations include the following:

- ○ Review the base SPAR model assumptions (e.g., event tree, fault tree, parameter basis) in the plant SPAR model manual before making changes.

- ○ ***Event Tree Modification (Base Case).*** This activity involves the modification or development of an event tree to incorporate additional details not included in the original model. Some considerations for event tree modifications include the following:
  - – Examples of additional details that may be added to the base case SPAR model include:
    - ▪ Additional top events that represent initiator recovery.

[60] Analysts should consult Idaho National Laboratory when making modifications to the base SPAR models.

        - Changes to an event tree linking rule that replace the default fault tree with a substitute fault tree.[61]
        - Completion of an undeveloped sequence in an event tree by linking the sequence end state to a transfer event tree.
        - New event tree that models a new initiating event or transfer tree.
    - Modifications to the SPAR model should be performed or reviewed by the SPAR model developer.
    - SAPHIRE instructions for creating and modifying event trees in the SPAR model are provided in the SAPHIRE training manuals.
    - A checklist for aiding in the review of event tree modifications is provided in Volume 3 of this handbook.

- ***Fault Tree Modification (Base Case).*** This activity involves the modification or development of a fault tree to incorporate additional details not included in the original model. This is typically in the form of a basic event added to a fault tree or a different fault tree linked to an event tree top event. Some considerations for fault tree modifications include the following:
    - Examples of additional details that may be added to the base case SPAR model include:
        - Actual failed or degraded components (focus of the analysis).
        - Alternative mitigating features present in the design.
        - Recovery actions to restore a failed/degraded component/system or recover from the actual or postulated initiator.
        - Observed human actions relevant to the risk significance of an actual initiating event.
        - Observed component/system interactions relevant to the risk significance of an actual initiating event.
        - Potential CCFs implied by the event (e.g., a maintenance error that fails one component and has the potential for failing additional components because of the use of a similar maintenance procedure or the same maintenance crew).
    - Modifications to the SPAR model should be performed or reviewed by Idaho National Laboratory.
    - SAPHIRE instructions for creating and modifying faults trees in the SPAR model are provided in the SAPHIRE training manuals.
    - A checklist for aiding in the review of fault tree modifications is provided in Volume 3 of this handbook.

- ***Initiating Event Frequency Parameter Update (Base Case).*** This activity involves the update, modification, or creation of an initiating event frequency parameter to incorporate additional details not included in the base case SPAR model. A modification

[61] Event tree linking rules are rules in the SPAR models that allow the user to replace one or more top events with substituted top events based on the logical conditions dictated by the rule. These rules also allow the user to assign flag sets to sequences based on the logical conditions dictated by the rule.

typically includes the update of the number of initiator occurrences (numerator) and the update of the associated reactor-years spanning the period of occurrences (denominator).

The new or modified parameter should reflect the nominal initiating event frequency in the modified base case SPAR model. Modifications to a parameter value that reflect the impact of the operational event will be performed in the next analysis step. Some considerations for parameter modifications include the following:

- Reasons to change or create an initiating event parameter in the base case SPAR model may include:
  - Update a parameter with more recent operational experience (i.e., extend the time period), because a parameter may be outdated.
  - Update a parameter with plant-specific operational experience, because the plant-specific operational experience justifies a higher or lower frequency.
  - Modify a generic, industry-average parameter by carefully screening the operational experience database for relevant events (data censoring), because
    - A unique plant-specific design feature makes the use of a generic, industry-average initiating event frequency questionable (e.g., may not represent the as-built, as-operated plant), given that sufficient data and operating experience exists to estimate a plant-specific probability,
    - A parameter definition was revised to reflect a modification to the SPAR model, or
    - A particular degraded condition exists for only a subset of the industry average initiator, so the operational experience database should be carefully screened for relevant events.
- Create a new parameter for a new initiating event category because the initiator type is unique for the plant or degraded condition in question (e.g., loss of a particular 120-volt or 480-volt alternating-current bus).[62]
  - Modifications to the SPAR model parameters should be performed or reviewed by analysts specializing in the data collection and parameter estimation.
- Caution must be exercised when screening (censoring) industry-wide data from a generic, industry-average parameter to reflect a unique plant-specific design feature or operational characteristic. Screening considerations must also be given to the denominator term of the parameter that represents the operational exposure. Some special considerations:
  - A plant-specific parameter estimate is more desirable than a censored industry-average estimate due to the judgments and assumptions involved with screening the operational exposure.
  - Censoring an event from a dissimilar plant usually requires the removal of operational exposure associated with that plant and other dissimilar plants where no failures were observed, but could occur.
  - A process for reducing the data necessary to calculate plant-specific initiating event frequencies and component failure probabilities are presented in

[62] A nominal initiating event frequency will be estimated and assigned for the modified base case SPAR model.

Sections 5.1 and 5.2 of NUREG/CR-6823, "Handbook of Parameter Estimation for Probabilistic Risk Assessment."

    - Initiating event frequencies used in SPAR models are typically based on the analysis methods and results from NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," Section 8 and Appendix D.[63] Updates will be posted on the Reactor Operational Experience Results and Databases Web page.
    - Other SPAR model parameters not based on NUREG/CR-6928 should be reviewed and updated as necessary. These parameters may be based on current plant-specific estimates from the plant PRA, outdated estimates from the Individual Plant Examination (IPE), or generic estimates from legacy sources (e.g., NUREG/CR-5750, "Rates of Initiating Events at U.S. Nuclear Power Plants: 1987–1995").
    - Refer to the plant SPAR model manual for the basis for parameter estimates.

  - SAPHIRE instructions for creating and modifying basic event parameters in the SPAR model are provided in the SAPHIRE training manuals.
  - Guidance for the use of support system initiating event (SSIE) models in ECA is provided in Section 11.
  - A checklist for aiding in the review of parameter modifications is provided in Volume 3 of this handbook.

- ***Basic Event Parameter Update—Component Failure Probability or Rate (Base Case).*** This activity involves the update, modification, or creation of a basic event parameter to incorporate additional details not included in the base case SPAR model. A modification typically includes the update of the number of failures (numerator) and the update of the associated number of demands or unit time spanning the period of failures (denominator).

  The new or modified parameter should reflect the nominal failure probability or rate in the modified base case SPAR model. Modifications to a parameter value that reflect the impact of the operational event will be performed on the current case SPAR model in the next analysis step. Some considerations for parameter modifications include the following:

  - Reasons to change or create a basic event parameter in the base case SPAR model may include:
    - Create a new parameter that represents the failed or degraded component.
    - Create a new parameter used in a fault tree that was revised to better represent the as-built, as-operated plant at the time of the operational event.
    - Update a parameter with more recent operational experience (i.e., extend the time period), because a parameter may be outdated.
    - Update a parameter with plant-specific operational experience because the plant-specific operational experience justifies a higher or lower failure

[63] Data used to estimate initiator frequencies are primarily from LERs for reactor trip events and the Monthly Operating Reports for reactor-critical years. The results were estimated using the Reliability and Availability Data System (RADS) calculator. Analysis methods are documented in NUREG/CR 6823.

    probability/rate.

  - Modify a generic, industry-average parameter by carefully screening the operational experience database for relevant events (data censoring) because
    - A unique plant-specific design feature makes the use of the generic, industry-average failure probability/rate questionable (e.g., may not represent the as-built, as-operated plant), given that sufficient data and operating experience exists to estimate a plant-specific probability, or
    - A parameter definition (e.g., component boundary, failure mode) was changed to fit a modification to the SPAR model.
- Check that changes in a basic event input parameter do 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 (e.g., CCF event)
  - Template event shared by basic events of a component group.
  - Basic event used in post-processing rules.
- Modifications to the SPAR model parameters should be performed or reviewed by analysts specializing in the data collection and parameter estimation.
- Caution must be exercised when screening (censoring) industry-wide data from a generic, industry-average parameter to reflect a unique plant-specific design feature or operational characteristic. Screening considerations must also be given to the denominator term of the parameter that represents the operational exposure. Some special considerations:
  - A plant-specific parameter estimate is more desirable than a censored industry-average estimate due to the judgments and assumptions involved with screening the operational exposure.
  - Censoring an event from a dissimilar plant usually requires the removal of operational exposure associated with that plant and other dissimilar plants where no failures were observed, but could occur.
  - A process for reducing the data necessary to calculate plant-specific initiating event frequencies and component failure probabilities are presented in Sections 5.1 and 5.2 of NUREG/CR-6823.
  - Failure probabilities used in SPAR models are based on the analysis methods and results from NUREG/CR-6928, Section 5 and Appendix A.[64] Updates to NUREG/CR-6928 will be posted on the Reactor Operational Experience Results and Databases Web page.
  - Other SPAR model parameters not based on NUREG/CR-6928 should be reviewed and updated as necessary. These parameters may be based on the plant-specific estimates from the plant PRA or IPE, or generic estimates from legacy sources (e.g., NUREG/CR-5750).

[64] Data used to estimate failure probabilities are primarily from Institute for Nuclear Power Operations Consolidated Events (ICES) database failure reports. The results were estimated using the RADS calculator. Analysis methods are documented in NUREG/CR-6823.

    - Refer to the plant SPAR model manual for the basis for parameter estimates.
  - SAPHIRE instructions for creating and modifying basic event parameters in the SPAR model are provided in the SAPHIRE training manuals.
  - A checklist for aiding in the review of parameter modifications is provided in Volume 3 of this handbook.
- ***Basic Event Parameter Update—CCF Probability (Base Case).*** This activity involves the update, modification, or creation of a CCF basic event parameter to incorporate additional details not included in the base case SPAR model. The new or modified parameter should reflect the nominal failure probability in the modified base case SPAR model. Modifications to a parameter value that reflect the impact of the operational event will be performed on the current case SPAR model in the next analysis step. Some considerations for parameter modifications include the following:
  - Reasons to change or create a CCF basic event parameter in the base case SPAR model may include:
    - Create a CCF parameter of a new common cause component group in a fault tree that was modified to include the following:
    - A component with the observed failure or degradation.
    - A better representation of the as-built, as-operated plant at the time of the operational event.
  - Update CCF parameters (e.g., Alpha Factor Model) with more recent operational experience (i.e., extend the time period), because a parameter may be outdated.
  - Modify a generic, industry-average parameter by carefully screening the operational experience database for relevant events (data censoring), because
    - A unique plant-specific design feature makes the use of the generic, industry-average CCF probability questionable (e.g., may not represent the as-built, as-operated plant), given that sufficient data and operating experience exists to estimate a plant-specific probability, or
    - A parameter definition (e.g., component boundary) or common cause component grouping was changed to fit a modification to the SPAR model.
  - Modifications to the SPAR model parameters should be performed or reviewed by analysts specializing in the CCF data collection and parameter estimation.
  - CCF probabilities used in SPAR models are based on "CCF Parameter Estimations, 2010" or recent report.
    - The data collection and analysis methods used to update CCF parameters in "CCF Parameter Estimations, 2010 Update" are based on NUREG/CR-6268, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding.”[65]
    - The Alpha Factor Method was used to estimate probabilities for all CCF events in the SPAR model. Refer to the plant SPAR model manual for details of the CCF model (Section 6) and CCF parameters (Appendix D) used in the SPAR model.

[65] Equipment failures that contribute to CCF events are identified during searches of LERs, Nuclear Plant Reliability Data System (NPRDS) failure reports, and ICES failure reports. The results were estimated using the CCF database calculator.

        Appendix B, “Basic Event Data Report,” in the SPAR model manual provides references to data sources in the table notes.

        - The priors used to calculate CCF parameters in the CCF database are provided in Section 2 of CCF Parameter Estimations, 2010 Update" labeled “No Data (Prior Only).” This is the result of calculating an application without any data, which is the same as calculating an application with all the events in the CCF database. These CCF parameters may be used for those cases where there is no reasonable set of data to approximate the intended event.

    - SAPHIRE instructions for creating and modifying CCF basic event parameters in the SPAR model are provided in the SAPHIRE training manuals.

    - A checklist for aiding in the review of CCF parameter modifications is provided in Volume 3 of this handbook.

- ***Basic Event Parameter Update—Human Error Probability (Base Case).*** This activity involves the modification or creation of a human failure event (HFE) to incorporate additional details not included in the base case SPAR model. The new or modified parameter should reflect the nominal failure probability in the modified base case SPAR model. Modifications to a parameter value that reflect the impact of the operational event will be performed on the current case SPAR model in the next task. Some considerations for parameter modifications include the following:

    - Reasons to change or create a new HFE in the base case SPAR model may include:

        - Create a new HFE in an event tree or fault tree that represents

            - Nonrecovery of the failed/degraded component or system,

            - Human failure that was observed during the operational event,

            - Deficiency in an operating procedure, or

            - Operator actions to initiate and control a mitigating system added to the SPAR model (that reflects the as-built, as-operated plant at the time of the operational event).

        - Modify a performance shaping factor (PSF) for a HFE that represents a unique plant-specific design feature makes the use of the generic SPAR model human error probability (HEP) value questionable (e.g., may not represent the as-built, as-operated plant).

    - Human actions included in the SPAR model consist of both pre-accident failures to restore systems following T/M, and post-accident failures to align systems, to control or operate systems, and to recover system hardware failures.

        - The following general naming scheme for the basic event component code and failure mode code for operator action events was adopted in SPAR models:

            XHE-XE   Failure to perform a manual operation

            XHE-XL   Failure to recover a hardware failure locally (outside of the control room) by manipulation of the failed component to achieve the desired alignment or operation of the component

            XHE-XM   Failure to manually align and actuate (a manually controlled system)

XHE-XO Failure to operate or control a system adequately to achieve required performance

XHE-XR Failure to restore from test or maintenance. Failure to restore events are considered pre-accident events and not evaluated using the formal human reliability analysis (HRA) procedures described in this section

    - Basic events used to model operator actions in SPAR models are generally generic (standardized) across plant designs [e.g., pressurized-water reactors (PWRs), boiling-water reactors (BWRs)] and represent human actions typically modeled in PRAs. A thorough HRA analysis was not performed to identify additional activities that have the potential to result in human failures. However, important human actions that were identified during benchmarking a plant SPAR model with the plant PRA were added to that SPAR model.

- The bases of HEP calculations for the HFEs used in the SPAR model are provided in the table notes in Appendix E of the plant SPAR model manual.[66]
- A description of the human reliability models used in SPAR models, including the treatment of dependencies between human action events, is provided in Section 9 of the plant SPAR model manual.
- The human reliability analysis method used to estimate most HEPs in SPAR models is the SPAR-H method (NUREG/CR-6883, “SPAR-H Human Reliability Analysis Method”).
    - The worksheet for each HFE that was estimated using the SPAR-H method is documented in Appendix E of the plant SPAR model manual.
    - Limitations to the SPAR-H and other HRA methods are evaluated in NUREG-1842, “Evaluation of Human Reliability Analysis Methods against Good Practices,” Section 3.8 and Table 4.1.
    - Additional guidance for applying SPAR-H in ECA is provided in Section 9.
- HRA “Good Practices” are documented in NUREG-1792, “Good Practices for Implementing Human Reliability Analysis.” “Good Practices” are provided for the following activities: HRA team formulation, pre-initiator HRA, post-initiator HRA (including recovery actions), modeling errors of commission, and HRA documentation.[67]
- SAPHIRE instructions for creating and modifying basic event parameters in the

[66] Most HEPs for the HFEs in the SPAR model were estimated using the SPAR-H method. Some HEPs for recovery actions (e.g., EDG, LOOP) were calculated using generic operating experience data. A few human action events may be based on legacy sources (e.g., IPE, older SPAR models, pre-SPAR models) with some HEPs assigned a value of TRUE.

[67] “Good Practices” are processes and individual analytical tasks and judgments that would be expected in an HRA in order for the HRA results to sufficiently represent the anticipated operator performance as a basis for risk-informed decisions. The HRA good practices documented in NUREG-1792 are of a generic nature; that is, they are not tied to any specific methods or tools that could be employed to perform an HRA. As such, the good practices support the implementation of Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” for Level 1 and limited Level 2 internal event PRAs with the reactor at full power. The decisions regarding which good practices are applicable—and the extent to which those practices should be met—depends on the nature of the given regulatory application. Therefore, certain practices may not be applicable for a given analysis, or their applicability may be of limited scope.

SPAR model are provided in the SAPHIRE training manuals.

  - A checklist for aiding in the review of HEP parameter modifications will be provided in a future revision to Volume 3 of this handbook.

- ***Solving the modified base case SPAR model.*** This activity involves the solution of modifications to the original base case SPAR model. The analyst should compare the results of the modified base case SPAR model to the original base case results to confirm expected changes in results, as well as to identify abnormalities. In addition, the review should ensure that the modified base case SPAR model reflects the plant-specific changes in previous steps and activities. Some considerations for solving the modified base case SPAR model include the following:

  - Important note - When updating base case model, ensure that any change case data (change sets) in SAPHIRE are not saved.
  - Solve the modified base case SPAR model using the same truncation probability as the original base case SPAR model.
  - Some considerations for reviewing cut set results include the following:
    - Compare the modified model sequence cut sets with those from the base case SPAR model to confirm model revisions.
    - Identify and review basic event parameters in cut sets that may have been truncated out in the original solution of the original base case SPAR model, but appeared in the solution of the modified base case SPAR model. Repeat Steps 2 and 3 for parameter values that have not been reviewed previously.
    - Check that no sequences that were conservatively or simplistically developed in the original base case SPAR model exist among the dominant sequences.
    - Check that basic events expected to be contributors to dominant cut sets are included in those cut sets.
    - Check for multiple recovery events in a cut set. Dependency between recovery events may need to be applied in some cases.
    - Check for mutually exclusive basic event combinations that may appear due to simplified model logic. Post-processing rules may be applied to eliminate the unwanted combinations.[68]
  - Using the risk achievement and risk reduction importance measures, check that probabilities of important basic events are reasonable and justifiable.
  - *Saving the modified base case SPAR model.* Save the modified base case SPAR model using a unique file name that associates the model with the event under analysis.
  - Each change to the original base case SPAR model should be documented including the basis and associated reference for each change. A suggested format for such documentation is in the plant SPAR model manual.
  - Changes to the original base case SPAR model that should be permanently reflected in the master plant SPAR model should be reported to Idaho National Laboratory.

[68] Use caution when deleting multiple train T/M combinations; such combinations have occasionally been observed in the operating experience data.

Changes may reflect errors found during the review, elaboration of underdeveloped event or fault trees, updates to base event parameters, and other updates that reflect the current as-built, as-operated plant.

- ▪ Document and report changes and suggestions for enhancement to Idaho National Laboratory using the "SPAR Model Change Logging System" that can be accessed from the SAPHIRE Users Group Web page.

□ **Step-4: Create a Change Case to Reflect the Event.** In this step, a change case refers to changes to basic event probability data in the base case SPAR model to reflect the failures, unavailabilities and other undesirable occurrences observed during an event. Modeling logic changes (e.g., modify an event or fault tree, adding a new basic event) to reflect the event were addressed in the previous step.[69] This step may include the following activities:

- ○ Identify the analysis boundary conditions,
- ○ Know where the basic event (or fault tree) is used in the SPAR model,
- ○ Adjusting initiating event probability,
- ○ Modeling initiating event nonrecovery probability,
- ○ Modeling failed SSCs,
- ○ Modeling degraded SSCs,
- ○ Modeling success,
- ○ Common-cause failure analysis in event assessment,
- ○ Modeling human errors,
- ○ Modeling unavailability due to test or maintenance, and
- ○ Modeling exposure time (condition duration).

Some considerations for modeling the event in the change case include the following:

- ○ ***Identify Analysis Boundary Conditions (Change Case).*** In this activity, the analyst defines the event boundaries in accordance with program-specific procedures (i.e., SDP, ASP, and MD 8.3). The boundaries of a risk analysis of an operational event are the starting and ending points in the event time line where postulated assumptions are analyzed.

  – *Initiating event analysis.* The observed time and cause of the event initiator should be used in modeling the severity of the event. The likelihood of the event initiator should not be modified to postulate a more severe outcome.

  For example, a tornado crosses the site causing a partial loss of offsite power to one vital bus. The likelihood of debris or the tornado slightly changing course (as tornados frequently do) causing a total loss of offsite power should not be postulated as an assumption.

  The analysis is typically concluded after the 24-hour PRA mission time for

[69] The base case and current case are two separate parts of a SAPHIRE project database. Base case data is stored in the data base files as a "permanent" record. Current case data is used to perform an analysis (e.g., cut set generation and quantification). The current case is created (via the Generate option) by applying change sets to base case data and is used for sensitivity or event analysis. All SAPHIRE calculations use the data stored in the current case. Current case can equal the base case in order to reproduce the original study stored in the base case.

sequences with stabilized plant conditions.

- *Condition analysis.* The observed time of discovery and cause of the component unavailability should be used in modeling the severity of the condition. The likelihood of a different cause or discovery time resulting in a more severe outcome should not be postulated in the analysis.

  For example, an unavailability of a component inside containment was discovered during an unplanned walkthrough prior to power operation. If the person had not been lucky to stumble upon this deficiency, the component unavailability would have not been detected until the scheduled inspection during the next outage. The likelihood of the unavailability remaining undetected should not be postulated as an assumption in this case.

  The analysis is typically concluded at the end of the condition exposure time (i.e., the time when the degraded or failed component is returned to service).

○ ***Know Where the Basic Event (or Fault Tree) Is Used in the SPAR Model (Change Case).*** Check that a proposed modification to an existing basic event or fault tree does not adversely impact the use of the same basic event or fault tree elsewhere in the SPAR model. The modification may not be appropriate in all sequences, especially for time-dependent recovery/repair actions.

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.

Some considerations include the following:

- Examples where a modification of a basic event can affect multiple parts of the model include:
  - Basic event used in different fault trees,
  - Basic event used in a compound event (e.g., CCF event),
  - Template event shared by basic events of a component group (e.g., motor-driven pump, motor-operated valve), and
  - Basic event used in post-processing rules.
- Examples of basic event parameter variables that could impact multiple parts of the model include:
  - Failure probability/rate,
  - Mission time,
  - Calculation type, and
  - Process flag.
- The same fault tree can be used in several event trees.
- A new basic event or fault tree may be easier to apply in the SPAR model.

○ ***Adjusting Initiating Event Probabilities (Change Case).*** The frequency of initiating events is specified as a probability in SPAR models. This probabilities of initiating events must be changed as follows:

- For an initiating event analysis, assign a probability of applicable initiator to 1.0. Set the initiating event probabilities of non-applicable initiating events to zero. This is performed automatically by SAPHIRE when using the ECA workspace. Treatment of initiating events differs between SDP, ASP, and MD 8.3 analyses. Refer to Section 8 for program-specific guidance.

  - For a condition analysis, revise the frequencies of the initiating events included in the model to the probability of each initiating event over the exposure time that the condition existed: p(initiator) = $1 - e^{-\lambda \times \text{exposure time}}$. This is approximately (λ × exposure time) for (λ × exposure time) < 0.1. This is performed automatically by SAPHIRE when using the ECA workspace.

- ○ ***Modeling Initiating Event Recovery Actions (Change Case).*** This activity involves the treatment of recovery from an initiator that resulted in an automatic or manual reactor trip. Several event trees in the SPAR model include a top event that represents the nonrecovery of a system-induced initiator.[70] More than one nonrecovery event may be modeled in an event tree, such as early and late recovery actions. The nominal nonrecovery probabilities used in the base case SPAR model were derived either from operational experience data or by human reliability analysis. The initiating event basic events used in SPAR models typically do not credit recovery (during data allocation) in the parameter frequency estimation.

  - For an initiating event analysis where a recovery action was not performed during the event, the appropriate basic event probability should be set to TRUE.
  - For an initiating event analysis where a recovery action was successful during the event, the appropriate basic event should remain at its nominal base case value.
  - The addition of a recovery action in the base case SPAR model is performed in Step 3 in this appendix.

- ○ ***Modeling Failed SSCs (Change Case).***[71] This activity involves the treatment of SSC failures observed during the operational event. A failure of a SSC is represented in the SPAR model by basic events based on failure modes [e.g., fail-to-start (FTS), fail-to-run (FTR), fail-to-open (FTO), fail-to-close (FTC)].

  Some considerations for modeling a failed SSC include the following:

  - See Section 3 for additional details.
  - A complete failure is modeled by setting the basic event probability of the appropriate failure mode to TRUE.
  - For SSC that are initially successful but failed during the mission (e.g., a pump that fails after running for four hours) a specific reliability analysis is required.
  - Do not credit an observed successful recovery action except probabilistically in a recovery analysis (see Step 7 in this appendix).

[70] Examples of event trees in SPAR models with nonrecovery actions may include LOOP, loss of main feedwater, loss of power conversion system, general transient, loss of instrument air, and loss of service water.

[71] A SSC is considered failed if it is unable to perform its intended function in accordance with the success criteria specified in the PRA (e.g., if its state is consistent with the state of components identified as failed in data analyses associated with the PRA). Loss of functionality is not necessarily related to inoperability as defined by the plant Technical Specifications (TS).

- ***Modeling Degraded SSCs (Change Case).***[72] This activity involves the treatment of a degraded condition observed during the operational event. The degraded condition is represented by basic events based on failure modes (e.g., FTS, FTR, FTO, and FTC). The probability of failure given the observed degradation usually involves the estimation of a higher failure probability that represents the degraded nature of the component. The expected higher failure probability estimate can be assessed using engineering judgment through expert elicitation. In some cases, the estimate may be derived through prior operating experience of the component.

  Some considerations for modeling a degraded SSC include the following:

  - The reasons for adjusting the nominal failure probability of a degraded SSC may include the following:
    - Degradation results in the reduction in functionality in at least one sequence.
    - Degradation did not reduce the functionality of the SSC at the time of discovery, but could have reduced functionality at some point in the condition duration due to the random nature of the degradation mechanism.
  - Reasons for not adjusting the nominal failure probability of a degraded SSC may include the following:
    - Degradation did not reduce the functionality of the SSC and the nature of the failure mechanism would not have reduced functionality at some point in the condition duration.
    - Degradation did not reduce the functionality of the SSC, but the SSC was declared inoperable, as defined by TS.
  - The basic event failure probability of a degraded SSC in the change case SPAR model would be redefined as a conditional probability of failure given the observed degradation. The conditional failure probability estimation should consider the following:
    - Probability of proceeding from the observed degraded state to a failed state.
    - Chance that the condition would not have been discovered before failure.
    - Expected duration of component failure before discovery (standby component).
  - For situations in which it is not clear if a component is failed, a detailed engineering analysis or an expert elicitation may be appropriate to provide a best estimate of component status.
    - Document engineering factors and bases for judgments that support the best-estimate functionality determination and associated failure probability.
    - Document uncertainties associated with the estimate for use in later sensitivity and uncertainty analyses.
  - A bounding estimate in an event analysis should not be considered unless it has little impact on the overall analysis results (e.g., bounding analyses can be used in a

[72] A degraded component can exhibit reduced performance but which still meets its success criteria as specified in the PRA. In addition, a degraded component can be an incipient failure that, if left un-remedied, could ultimately lead to a degraded or unavailable state.

screening analysis to eliminate an event from further consideration).[73]

- ***Modeling Success (Change Case).*** This activity involves the treatment of SSC and human actions that were observed during the operational event to have operated and performed successfully throughout the PRA mission time. In such cases, the failure probabilities of associated basic events will remain at the nominal failure probabilities as modeled in the base case SPAR model.

  For example, an injection pump that operated successfully (start and run) for the 24-hour mission time during the actual event or during a post event test would not be modeled by an overall failure probability of zero. The nominal failure probabilities would be retained for the associated basic events.

  Some considerations for modeling a successful SSC and human actions include the following:

  - SSCs that are observed to operate successfully or that are not challenged during the event use a failure probability equal to the nominal failure probability of the SSC.
  - Human actions that were observed accomplished successfully or that were not challenged during the event use a HEP equal to the nominal value.

- ***CCF Analysis in Event Assessment (Change Case).*** This activity involves the treatment of component failures and degradations with potential common-cause failure implications that were observed during the operational event. The common-cause plug-in modules in SAPHIRE automatically calculate CCF probabilities for a number of special cases often encountered in events analysis. Refer to Section 5 for specific guidance on this topic.

- ***Modeling Human Errors (Change Case).*** This activity involves the treatment of deficiencies in human performance and other performance issues that were observed during the operational event. An adjustment may be made to one or more HFE modeled in the original base case SPAR model. The probability of failure given the observed deficiency or performance issue usually involves the adjustment of a PSF to a higher level.

  Some considerations for modeling human errors include the following:

  - An observed human error is modeled by setting the appropriate HFE in the SAPHIRE change case to TRUE.
  - An adjustment to HEP of a HFE based on observed performance deficiencies can be performed using one of the publically available NRC HRA methods, such as:
    - The SPAR-H method as documented in NUREG/CR-6883, Section 9 of this handbook, and INL/EXT-10-18533, “SPAR-H Step-by-Step Guidance,” or
    - The second-generation HRA method called a Technique for Human Event Analysis (ATHEANA) described in NUREG-1624, “Technical Basis and Implementation Guide for a Technique for Human Event Analysis,” or
    - A combination of both of the above methods with the ATHEANA method used in the qualitative front-end portion of the HRA and SPAR-H method used to quantify

[73] If the failure probability of one component (e.g., pump A FTS) is changed to a different value of the other components in the CCCG, the SAPHIRE CCF plug-in module will recalculate the CCF probability for that CCCG using the maximum of the component’s input probabilities.

the HEP with contextual information derived from ATHEANA process.

  – If ATHEANA or another HRA method is used instead of SPAR-H, the HEP used in the base case SPAR model should be re-evaluated using the alternate method. Modifications to the base case SPAR model are performed in the Step 3 of this appendix.

  – Request assistance from a human reliability analyst.

- ○ ***Modeling Unavailability due to T/M.*** This activity involves the treatment of a system, train, or component that was disabled for T/M activity during the operational event.

  – Treatment of a component in T/M is application specific. Refer to the appropriate program-specific procedure (i.e., SDP, ASP, and MD 8.3) for modeling rules.

  For example, in an ASP analysis, the T/M basic event is set to TRUE for observed T/M activities during the operational event or not adjusted from the base case (nominal) value for no observed T/M activities. In an SDP analysis, T/M basic event is not adjusted from the nominal value regardless of observed T/M activities, unless the T/M activity can be contributed to the same performance deficiency (PD) under assessment.

- ○ ***Modeling Exposure Time (Condition Duration).*** The exposure time (sometimes known as failure or condition duration) is used by the SAPHIRE code in a condition analysis to model the duration over which the risk of the condition (i.e., failure, degradation) is measured. After SAPHIRE completes the cut set evaluation, it will apply the exposure time of the failure or degradation.

  Some considerations for modeling exposure time include the following:

  – Refer to Section 2 for details on when to apply full exposure time (*T*) or half exposure time (*T/2*).

  – Failure durations should be based on the nature of the failure.

  – The maximum exposure time (T) in a condition analysis is usually limited to one year, unless specified differently in program-specific procedure (i.e., SDP, ASP, MD 8.3).

□ **Step-5: Estimation of Event Significance (Initial Model Solution).** Estimation of the significance of an operational event is an iterative process. This process involves an initial solution that identifies likely significant sequences and cut sets. A thorough review of the sequences and cut sets is performed to identify additional plant and operational information that should be gathered. In addition, the review should identify potential modeling errors that should be resolved in order to have confidence in the analysis results. The review is followed by additional model elaboration, modification, and solution cycles (Steps 2–4 of this appendix, respectively) to develop a best estimate of the event significance.

This step may include the following activities:

- ○ Treatment of recovery events,
- ○ Analysis truncation,
- ○ Initiating event analysis,
- ○ Analysis of an initiating event with an observed failure,
- ○ Condition analysis, and
- ○ Analysis of concurrent conditions.

Some considerations for solving the model include the following:

- ***Treatment of Recovery Events.*** Set basic events included in the model that represent the recovery of components, if modeled, to 1.0. However, if recovery was not feasible, then set the recovery event to TRUE

  Component recovery is added to the model in a separate recovery analysis following the model solution. Setting recovery events to 1.0 instead of TRUE will allow the review of cut sets associated with the recovery action.

- ***Analysis Truncation.*** The runtime associated with a particular analysis is a function of, among other things, the truncation value. The analyst must fully understand the implications on the results when establishing the analysis truncation value.

  - Setting the analysis truncation equal to the base case truncation will assure that all the sequences and minimal cut sets contained in the base case are captured in the analysis results (assuming that the analyzed event involves equipment or human action degradation or failure). This practice should be given primary consideration. However, due to the size of the model and the nature of the analysis, it will not always be possible to set the analysis truncation equal to the base case truncation.
  - For a condition assessment, setting the analysis truncation equal to the base case truncation times the condition duration should result in the analysis case retaining a comparable number of sequences and minimal cut sets as in the base case. It is suggested that wherever possible to be somewhat conservative.

    For example, if the condition duration is 72 hours, raise the truncation by a factor of 10, not 100.
  - For an initiating event assessment, setting the analysis truncation equal to the base case truncation times the change in initiating event frequency should result in the analysis case retaining a comparable number of sequences and minimal cut sets as in the base case.

    For example, if the transient initiating event frequency is 1E-4/year, then setting the analysis truncation four orders of magnitude higher should keep the analysis results about the same size as the base case in terms of numbers of sequences and minimal cut sets retained.
  - Sequences with negative event importance should be reviewed. Sometimes they are valid, but only if there are complemented events in the minimal cut sets impacted by the event being analyzed.
  - If the event being modeled is not showing up in the minimal cut sets, then the base case SPAR model may require to be resolved at a lower truncation value. These cut sets may be truncated out in the base case SPAR model results.
  - Truncation values of 1×10^{-11} generally provide a sufficient number of minimal cut sets to capture the vast majority of the core damage frequency or conditional core damage probability without causing excessive runtimes.
  - Refer to the plant SPAR model manual, “Notes to Analysts,” for additional details on truncation values.

- ***Initiating Event Analysis.*** For initiating event assessments, the initiating events in the SPAR model must be modified in the change case to reflect the event in question. First, set those initiators that did not occur to FALSE (or a probability to zero). Second, set the initiator that did occur to TRUE (or a probability of 1.0).

- ○ ***Analysis of an Initiating Event with an Observed Failure.*** This activity involves the consideration of two separate risk analysis of an initiating event with an observed failure of a risk-important SSC. First, an initiating event analysis should be performed with the observed failure to arrive at a conditional core damage probability (CCDP). Second, a condition analysis (with the initiating event probabilities remain at the base case or nominal value) should be performed to determine the increase in core damage probability (ΔCDP) of the SSC failure over the exposure time of the SSC unavailability. The higher risk contribution should be used in accordance with program-specific procedures (i.e., SDP, ASP, and MD 8.3).

  For example, a failure of a turbine-driven auxiliary feedwater pump may be more important in a postulated station blackout than an actual general transient, if the pump was determined to be unavailable for a longer period of time. However, one precursor would be counted in ASP for this example.

- ○ ***Condition Analysis.*** For a condition analysis, the ΔCDP is calculated by first solving the CCDP based on the observed condition and exposure time. Then the base case (baseline) core damage probability (CDP) is subtracted from the CCDP result. This subtraction function is performed by SAPHIRE.

- ○ ***Analysis of Concurrent Conditions.*** This activity involves the treatment of concurrent multiple conditions involving two or more degraded and/or failed SSC observed in an operational event. One of the conditions may involve an unavailable component or train due to T/M activity. This activity includes the summation of exposure time segments of all applicable conditions.

  - – Refer to the program procedure (i.e., SDP, ASP, MD 8.3) for application-specific rules regarding the treatment of concurrent conditions.

    For example, in an SDP analysis, only concurrent conditions resulting from the same PD are considered in one analysis; otherwise, each PD is treated in a separate SDP analysis.

  - – Calculate the ΔCDP of each part of the overlap separately, if appropriate for the analysis application. Sum the ΔCDP for each part to calculate the overall condition analysis importance. This summation is performed by the analyst, not automatically by SAPHIRE.

  - – Refer to Section 2.10 for examples of exposure time modeling of multiple conditions.

□ **Step-6: Review of Initial Model Solution Results.** The results developed in previous step are the initial set of results without recovery actions. These results should be reviewed by the analyst to ensure their correctness. The cut sets associated with both dominant and non-significant sequences are reviewed to ensure no errors have been made during the modifications of the base case and current case SPAR models.

This step may include the following review activities:

- ○ Documentation,
- ○ Change case inputs,
- ○ Condition exposure time,
- ○ Truncation value,
- ○ Cut sets,
- ○ Multiple operator actions,
- ○ Importance measures,
- ○ Model uncertainties, and

- Reasonableness review.

Some considerations for the review of initial results include the following:

- ***Documentation Review.*** Check that the documentation of model modifications matches the modified base case SPAR model. Review the following modifications:
  - Success criteria,
  - Event trees,
  - Event tree linking rules,
  - Event tree process flags,
  - Fault trees,
  - Post-processing rules,
  - Basic events, and
  - Parameter values.

- ***Change Case Inputs Reviews.*** Check for the proper selection and input of parameter variables in the basic event that represents the failure or unavailability. Basic event parameter variables to check include:
  - Failure probabilities/rates,
  - Mission times,
  - Calculation types, and
  - Process flags.

  Other considerations include:

  - Except for recovery parameter(s) that were temporarily changed to 1.0 in the previous step, check that the basic event(s) of failed component(s) is set to TRUE instead of 1.0.
  - Check that a modification to a basic event parameter variable does not adversely impact the use of the same basic event elsewhere in the SPAR model. Examples where a modification of a basic event 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 post-processing rules (see below).
  - 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 basic 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 conditioned disallowed by TS, or failure to apply a human error dependency.

- ***Condition Exposure Time Review.*** Check the exposure time of the failed or degraded SSC condition.

- ***Truncation Value Review.*** Check that the truncation probability used in the model solution is sufficient for the application.

- ***Cut Set Reviews.*** Using the nominal cut sets from the original and modified base case SPAR models as guides to expected cut set structure, confirm that the results developed from the current case model are consistent with the failures, unavailabilities, and off-normal conditions that were observed during the operational event.[74]
    - Compare the modified model sequence cut sets with those from the base case SPAR model to confirm model revisions.
    - Check that the results are consistent with the failures, unavailabilities, and off-normal conditions that were observed in the operational event.
    - Check that the probabilities for sequences that are adversely impacted by the condition or event are higher in probability than in the base case SPAR model.
    - Check for sequences that were conservatively or simplistically developed in the base case SPAR model that exist among the dominant sequences.
        - If these do exist, it is recommended that the fidelity of such sequences be increased to a level consistent with the significant sequences in the base case SPAR model.
        - Alternately, clearly identify those sequences that are likely conservative in the analysis documentation.
    - Check that no basic events impacted by a component failure appear in an unmodified form unless this is appropriate for the event.
    - 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.
    - Check that basic events expected to be contributors to dominant cut sets is included in those cut sets.
    - Check that new or modified basic events are appropriately reflected in the cut sets, as appropriate (e.g., the CCF probability associated with a failed component).
    - Check and evaluate multiple recovery events in a cut set.
    - Check for mutually exclusive basic event combinations that may appear due to simplified model logic.

- ***Multiple Operator Actions Reviews.*** Check for multiple operator actions in cut sets to verify that dependencies have been appropriately applied in the human error probabilities.

- ***Importance Measures Reviews.*** Using the risk achievement and risk reduction importance measures associated with the conditional cut sets, check that:
    - Basic events expected to be important based on the failures and off-normal conditions observed during the condition or event are, in fact, important.
    - Probabilities of important basic events are reasonable and justifiable.

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

[74] Keep in mind that recovery event of failed or degraded SSC may have been set to 1.0 in a previous step.

documentation.

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

- ○ Return to previous analysis steps to resolve any discrepancies.

□ **Step-7: Recovery Analysis and Model Solution.** This step involves a recovery analysis, SPAR model modifications to reflect the recovery analysis, and model solution with recovery applied. In Step 5 of this appendix, the initial model solution was ran with the nonrecovery probability set of 1.0 for the purpose of identifying cut sets for potential recovery applications. Recovery analysis addresses the potential recovery of lost functions and human errors, and repair of failed components prior to core damage.

Recovery/repair actions can be added at various levels in the SPAR model: event tree, fault tree, sequence, or cut set. The appropriate level depends on how narrow the application of the recovery/repair action is desired. All applications will require a basic event in a fault tree, either the use of an existing basic event or the creation of a new basic event. A post-processing rule can also be developed or an existing rule edited to replace the recovery/repair basic event with time-dependent probabilities at the cut set, sequence, or event tree top event level. Some considerations for crediting and applying recovery include the following:

- ○ Refer to Section 6 additional information on modeling recovery actions.

- ○ ***Solve and Review Cut Sets.*** Recover cut sets that constitute at least 99% of the total CDP.
  - – Re-sort cut sets as necessary to identify those that rank in the upper 99th percentile (as cut sets are recovered their relative significance will be reduced).
  - – Refer to the previous analysis step on the review of initial results for items to review.

□ **Step-8: Review of Final Analysis Results.** The results developed from the previous step are the final recovered results of the analysis. These results are reviewed by the analyst to ensure their correctness prior to event documentation. As with the initial model solution, the cut sets that are associated with both dominant and non-significant sequences are reviewed to ensure no errors have been made during the iterative SPAR model modification process. Some considerations for reviewing the final analysis include the following:

- ○ ***Inputs and Assumptions.*** Step back from the analysis.
  - – Review the event specifics and chronology developed in Step 1 of this appendix.
  - – Check the basis for each assumption.
  - – Check for the appropriate input from inspectors and methods experts.
  - – Re-check the base case SPAR model revision (for just released newer revision).

- ○ ***Plant Design and Operations (As-Built, As-Operated Plant).*** Ensure that the analysis results reflect the as-built, as-operated plant for those sequences impacted by the operational event. Increasing failure probability of basic events may cause underdeveloped cut sets to rise to the top in risk significance.

- ○ ***Documentation.*** If not already performed in a previous step, compare the documentation associated all model modifications with the base case SPAR model and current case.

- ○ ***Sequences and Cut Sets.*** Review the final list of significant sequences and cut sets in accordance with the review items in Step 7 of this appendix.

- ○ ***Results.*** Confirm that the analysis results are consistent with all of the information available concerning the event.
  - – Does the analysis adequately characterize the event?
  - – Do the analysis results make sense?

- ○ Return to the appropriate analysis step to resolve any discrepancies.

□ **Step-9: Sensitivity and Uncertainty Analyses.** Sensitivity and uncertainty analyses provide estimates of the variability in the risk estimate due to data variability, model inaccuracy, and modeling assumptions included in the event analysis.

- ○ ***Uncertainty Analysis.*** A typical uncertainty analysis addresses the impact of data variability in the basic event parameters included in the model (e.g., initiating events frequencies, failure probabilities, unavailability probabilities, CCF probabilities, human error probabilities, nonrecovery probabilities).

  Two sampling techniques are provided in SAPHIRE code for estimation of the variability (due to the uncertainties in the basic event probabilities) of either a fault tree top event probability or an event tree sequence frequency: Monte Carlo simulation and Latin Hypercube simulation. Either is adequate for most ASP and SDP analyses. Monte Carlo simulation methods are generally used to perform uncertainty analysis.

- ○ ***Sensitivity Analysis.*** A typical sensitivity analysis addresses the impact of alternate analysis assumptions and technical issues in SPAR models. Analysis assumptions are related to the uncertain specifics of the operational event, usually the reliability of a degraded component. Technical issues with SPAR models include known areas of uncertainties, such as CCF modeling and human reliability analysis modeling, and other potential modeling issues that have been identified through quality review process of the SPAR model. These technical issues are generic to plant classes and SPAR models.

Some considerations include the following:

- ○ ***Key SPAR Model Assumptions and Technical Issues.*** Refer to Section 2.2 of Volume 3 of this handbook for a list of key SPAR model assumptions and technical issues.

- ○ ***Sensitivity Analysis.*** Sensitivity analyses should be performed on assumptions developed in Steps 1 and 2 of this appendix, as well as key SPAR model assumptions and technical issues that potentially drive the risk.
  - – In the analysis documentation, a detailed discussion of the assumptions that

significantly impact the results should be provided.

- – If an uncertainty analysis has been performed, address assumptions that result in point estimates outside the 5th and 95th percentile uncertainty bounds calculated below.

○ ***Uncertainty Analysis.*** A Monte Carlo uncertainty analysis should be performed using the recovered cut sets that represent the final analysis results.

- – Ensure that all basic events, including nonrecovery actions added to the initial analysis cut sets, are defined in terms of probability distributions (except basic events assigned a probability of 1.0).[75]
- – The SAPHIRE instructions for performing an uncertainty analysis of SPAR model parameters can be found in the SAPHIRE training manuals.
- – Utilize a sufficient number of trials to insure accuracy (at least 10,000 trials are recommended). Confirm that the mean estimate developed in the Monte Carlo analysis is consistent with the point estimate developed from the cut sets.
- – Include the results of the Monte Carlo analysis in the analysis documentation. Discuss the impact of the estimated range in risk significance on the overall conclusions of the analysis.

○ ***Documentation of Results.*** Care should be taken when documenting the results of a sensitivity analysis to avoid the appearance of multiple results or conclusions. Sensitivity analysis results used to support an assumption or conclusion should be referenced qualitatively (e.g., “generally in agreement,” “minimal effect”). Sensitivity results provided as an input to be considered in a final decision of an application should be discussed in context of analysis results used for the record.

□ **Step-10: Analysis Documentation.** Documentation of analyses should use proper PRA terminology, identify key uncertainties and sensitivities and their significance, and be sufficiently complete and scrutable to permit a quality assurance review. The analysis document not only provides assumptions and results of the operational event, but also the descriptions and bases of SPAR model modifications that deviate from the plant-specific SPAR model manual. Some considerations of information to include in an analysis document include the following:

○ ***Bases.***

- – Facts about the condition or event should have a referenced source.
- – Each assumption should be clearly linked to the fact(s).
- – Each modification to the base case SPAR model and current case should be linked to the associated assumption or fact.

○ ***Facts.***

- – Facts most important to the risk should be stated first.
- – For initiating event analyses, all off-normal conditions should be stated.

[75] Use caution that distributions for high-probability basic events do not include tails with significant percentages above 1.0.

  - Facts not used in the analysis should be noted so that the reviewer does not have to guess if considerations were missing.

- ***Assumptions.***
  - All assumptions, including unknowns, should be clearly stated.
  - Bounding assumptions and screening values should be clearly noted as such.
  - Important assumptions should be highlighted up front so that the reviewer can focus their review.

- ***Modifications.***
  - List old and new values, including the basis for the change (linked to the assumption and fact).
  - Describe event tree and fault tree modifications so that they can be independently reproduced.
  - Attach markups of effective pages from the plant SPAR model manual, such as:
    - Fault tree and event tree figures and descriptions,
    - Parameter tables,
    - HRA worksheets, and
    - Plant diagrams (note: avoid physical layout and floor plans that may be classified as sensitive unclassified non-safeguards information).
  - Document the revisions and dates of the SPAR model and SAPHIRE code.

- ***Results.***
  - Summarize the results, including the results of sensitivity and uncertainty analyses, as appropriate.
  - Attach the SAPHIRE printout, as appropriate.

- ***References.***
  - Sources of plant information used to modify the base case SPAR model (e.g., procedures, system descriptions, diagrams, technical specifications).
  - Sources of event-related information used in the analysis (e.g., inspection report, licensee=s root cause assessment, LER).
  - Verbal sources of plant and event-related information.
  - Preliminary reviews of methods applications and enhancements.