Risk Assessment of Operational Events

Handbook

Volume 1 – Internal Events

Exposure Time Modeling – Failure Modeling
Mission Time Modeling – T/M Outage Modeling – Recovery Modeling
Multi-Unit Considerations – Analysis Road Map

Revision 1.03

August 2009

SDP Phase 3 ● ASP ● MD 8.3

TABLE OF CONTENTS

ACRONYMS

ac	alternating current
AFW	auxiliary feedwater
ASP	accident sequence precursor
BWR	boiling water reactor
CCF	common-cause failure
CCCG	common cause component group
CDF	core damage frequency
CDP	core damage probability
dc	direct current
EDG	emergency diesel generator
EFW	emergency feedwater
EOP	emergency operating procedure
EPIX	Equipment Performance and Information Exchange (database)
FTR	failure to run
FTS	failure to start
GEM (code)	Graphical Evaluation Module (code)
gpm	gallons per minute
HEP	Human error probability
HFE	human failure event
HPCI	high-pressure core injection
HPI	High-pressure injection
HRA	human reliability analysis
HVAC	heating, ventilation and air conditioning
IA	Instrument air
IMC	Inspection Management Chapter
LER	Licensee Event Report
LOCA	loss-of-coolant accident
LOIA	loss of instrument air
LOOP	loss of offsite power
LPSI	low-pressure safety injection
MD 8.3	Management Directive 8.3
MFW	main feedwater
NPSH	net positive suction head
NR	non-recovery
PCS	power conversion system
PI	performance indicator

PRA	probabilistic risk assessment
PWR	pressurized water reactor
RADS	Reliability and Availability Data System
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
SSC	structures, systems and/or components
SSU	safety systems unavailability
T	exposure time
T/M	test or maintenance
TS	Technical Specifications
TDAFW	turbine-driven auxiliary feedwater

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 could 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.

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 8.3). 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," 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 the risk analysis of operational events. It is assumed that the analysts using this handbook have received PRA training at the SRA qualification level. Analysts using this handbook should be familiar with the risk analysis of operational events, 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 NRC course "Risk Assessment in Event Evaluation" (Course Number P-302) or has related experience.

1.4 Handbook Content

The revised handbook includes three volumes, designed to address Internal Events (Volume 1), External Events (Volume 2), and SPAR Model Reviews (Volume 3). 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 Determination and Modeling
  - Failure Determination and Modeling
  - Mission Time Modeling
  - Test and Maintenance Outage Modeling
  - Modeling Recovery and Repair Actions in Event Assessment
  - Multi-Unit Considerations Modeling

  In addition, the appendices provide further guidance on the following analysis topics:

  - Road Map – Risk Analysis of Operational Events
  - Quick Reference Guide – SAPHIRE Version 7

  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 low-power and 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.

[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.

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 PRA Review Manual (NUREG/CR-3485, Ref. 1-1), the PRA Standard [ASME RA-S-2005 (Ref. 1-2) and Regulatory Guide 1.200 (Ref. 1-3)], 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.

1.5 Companion References to the Handbook

Guidance in the three volumes of the handbook often refers to other references, as applicable to the application. A bibliography of current technical references used in the risk analysis of operational events is provided in Volume 3, in which most of the documents are referenced in individual sections throughout the handbook.

Key companion references that are an extension to this handbook include:

- PRA Standard (Refs. 1-2 and 1-3)
- NUREG/CR-6823, "Handbook of Parameter Estimation for Probabilistic Risk Assessment" (Ref. 1-4)
- NUREG-1792, "Good Practices for Implementing Human Reliability Analysis (HRA)" (Ref. 1-5)
- NUREG-1842, "Evaluation of Human Reliability Analysis Methods Against Good Practices" (Ref. 1-6)
- NUREG/CR-6883, "SPAR-H Human Reliability Analysis Method" (Ref. 1-7)
- NUREG-1624, Rev. 1, "Technical Basis and Implementation Guide for A Technique for Human Event Analysis (ATHEANA)" (Ref. 1-8)
- NUREG-1880, "ATHEANA User's Guide" (Ref. 1-9)

- NUREG/CR-6850, "EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Volume 2: Detailed Methodology" (Ref. 1-10)
- Handbook for Phase 3 Fire Protection (FP) Significance Determination Process (SDP) Analysis (Ref. 1-11)
- Basic SAPHIRE training manual (Ref. 1-12)
- Advanced SAPHIRE training manual (Ref. 1-13)
- 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.

- ***Revision 2 plans.*** Current plans for Revision 2 of the handbook will include the following additional method guides and tutorials:

  Methods

  - Common-Cause Failure Analysis in Event Assessment
  - Human Reliability Analysis in Event Assessment
  - Parameter Estimation and Update Methods in Event Assessment
  - Convolution of Failure to Run Parameters Method
  - Uncertainty Analysis Method in Event Assessment
  - Simplified Expert Elicitation Method in Event Assessment

  Tutorials and examples

  - Internal Events Modeling of Conditions and Initiating Events – Examples
  - Quick Reference Manual – SPAR Models
  - Tutorial - Common-Cause Failure Analysis in Event Assessment
  - Tutorial - NRC's Risk Databases and Calculators

- ***Future volume.*** One additional volume is planned in the near future:

  - Risk Analysis of Shutdown Events

1.7 Questions, Comments, and Suggestions

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

From internal NRC staff and NRC contractors:

- Volume 1, Internal Events
  - Don Marksberry, 301-215-7593, Don.Marksberry@nrc.gov
  - See-Meng Wong, 301-415-1125, See-Meng.Wong@nrc.gov
  - Chris Hunter, 301-415-7575, Christopher.Hunter@nrc.gov
- Volume 2, External Events
  - Selim Sancaktar, 301-215-7572, Selim.Sancaktar@nrc.gov
- Volume 3, SPAR Model Reviews
  - Peter Appignani, 301-251-7608, Peter.Appignani@nrc.gov

From external NRC stakeholders (e.g., public, licensees):

- All handbook volumes; Significant Determination Process
  - Paul Bonnett, 301-415-4107, Paul.Bonnett@nrc.gov

1.8 References

1-1. U.S. Nuclear Regulatory Commission, “PRA Review Manual,” NUREG/CR-3485, September 1985. (ADAMS Accession Number ML063550234)

1-2. American Society of Mechanical Engineers, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME RA-S-2005, 2005.

1-3. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” Revision 1, January 2007. http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-200/01-200r1.pdf

1-4. U.S. Nuclear Regulatory Commission, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” NUREG/CR-6823, September 2003. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6823/

1-5. U.S. Nuclear Regulatory Commission, “Good Practices for Implementing Human Reliability Analysis,” NUREG-1792, April 2005. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1792/

1-6. U.S. Nuclear Regulatory Commission, “Evaluation of Human Reliability Analysis Methods Against Good Practices,” NUREG-1842, March 2006. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1842/

1-7. U.S. Nuclear Regulatory Commission, “The SPAR-H Human Reliability Analysis Method,” NUREG/CR-6883, August 2005. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6883/

1-8. U.S. Nuclear Regulatory Commission, “Technical Basis and Implementation Guide for A Technique for Human Event Analysis (ATHEANA),” NUREG-1624, Rev. 1, May 2000. http://www.nrc.gov/reading-rm/doc-collections/nuregs/pubs/

1-9. U.S. Nuclear Regulatory Commission, “ATHEANA User’s Guide,” NUREG-1880, June 2007. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1880/

1-10. U.S. Nuclear Regulatory Commission, “EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Volume 2: Detailed Methodology,” NUREG/CR-6850, September 2005. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6850/

1-11. U.S. Nuclear Regulatory Commission, “Handbook for Phase 3 Fire Protection (FP) Significance Determination Process (SDP) Analysis,” December 2005. (ADAMS Accession Number ML053620267)

1-12. Idaho National Laboratory, “SAPHIRE Basics - An Introduction to Probabilistic Risk Assessment via the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software,” January 2005 or current revision.

1-13. Idaho National Laboratory, “Advanced SAPHIRE - Modeling Methods for Probabilistic Risk Assessment via the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software,” March 2005 or current revision.

2.0 Exposure Time Determination and Modeling

2.1 Definitions

- ***Exposure time.*** Exposure time (*T*) is the duration period of the failed or degraded structure, system or component (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 to be available during shutdown.

    - Note: The SAPHIRE Graphical Evaluation Module (GEM) code (Version 7) uses the term "event duration time" (in hours) instead of *exposure time*.

- ***Repair time.*** The PRA Standard defines *repair time* as ". . . the period from identification of a component failure until it is *returned to service*. No standard regulatory definition exists for *returned to service*. Therefore, for the purpose modeling of exposure time in the risk analysis of operational events, *returned to service* means the time at which any clearance tagging associated with the repair is removed and the component is considered capable of performing its intended function <u>following</u> successful post-maintenance surveillance testing. [2]

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

    - For Management Directive (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.

[2] 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.

- An *operation* can include 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.

2.2 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. See ASP analysis 336/01-005 from the ASP database (Ref. 2-1).
  - 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. See ASP analysis 395/00-006 from the ASP database (Ref. 2-1).
  - 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. See ASP analysis 483/01-002 from the ASP database (Ref. 2-1).

2.3 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 functionally 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). See ASP analysis 483/01-002 from the ASP database (Ref. 2-1).

2.4 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. 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 (24 hours).

- ***∑(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 32 hours of run time during surveillance tests prior to run failure on September 30. Inception of failure mechanism was known to be January 1. Exposure time is 6 months based on the 24 hours of run time (PRA mission time) prior to failure. Note: The 6 months exposure time would apply in this case even if the inception date was not known.

Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
4 hrs	4 hrs	4 hrs	4 hrs	4 hrs	4 hrs	4 hrs	4 hrs	4 hrs
←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.

  Note: 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 (see above).

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. Exposure time is 9 months.

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

- Repair time is included in the exposure time.

2.5 Exposure Time for Continuous Component Operation Failures

- For failure of a component that is normally in continuous operation while at-power (e.g., service water pump), the exposure time should be the PRA mission time (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. See ASP analysis 390/04-005 from the ASP database (Ref. 2-1).

2.6 Exposure Time > One Year

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

  Examples where an extended exposure time (T) is limited to one year:

  - The “t/2 + repair time” period greater than one year.

- The "t + repair time" period greater than one year.

- Examples of conditions that may have existed for longer than one year:
  - Design deficiency of a structure, system, or component that has been present since installation, modification, or construction. See ASP analyses 266/01-005, 247/02-010, and 287/02-015 from the ASP database (Ref. 2-1).
  - Construction debris found in a pump suction source not normally tested or inspected (e.g., containment sump line). See ASP analysis 400/01-003 from the ASP database (Ref. 2-1).
  - Calculation error discovered during a design audit. See ASP analyses 269/98-004 and 335/97-011 from the ASP database (Ref. 2-1).

2.7 Exposure Time for Concurrent Conditions

- This category includes the summation of exposure time segments of concurrent multiple equipment or functional degradations.
- The treatment of concurrent conditions is specific to the analysis application. Refer to the program-specific procedure (i.e., SDP, ASP, MD 8.3).
- Attachment 2-1 provides examples of exposure times for concurrent conditions.

2.8 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.
- Attachment 2-1 provides examples of exposure times for T/M contributions.

2.9 References

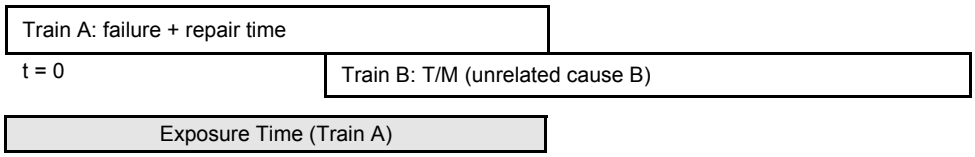
2-1. U.S. Nuclear Regulatory Commission, "Accident Sequence Precursor Database," https://nrcoe.inel.gov/secure/aspdb/, August 2007. *(NRC internal Web site - available to NRC staff only)*

This page intentionally left blank

Attachment 2-1. Examples of Exposure Times for Concurrent Conditions

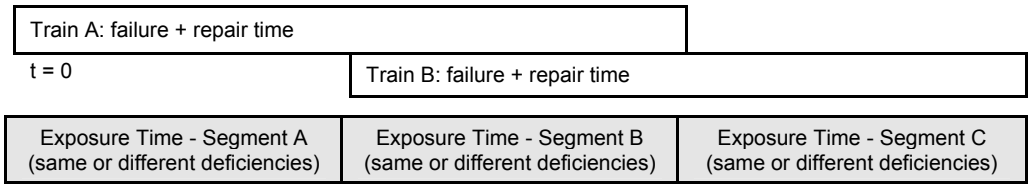
- **Case A - Condition analysis of one failure.** Failure of one train and unavailability of another train with overlapping exposures (same or different systems):

  If the cause for the test or maintenance (T/M) outage of Train B is NOT related to the failure of Train A, then the exposure time only applies to the Train A failure.



- **Case B - Condition analysis of two failures with overlap.** Failure of one train and a failure in another train with overlapping exposure times (same or different systems):

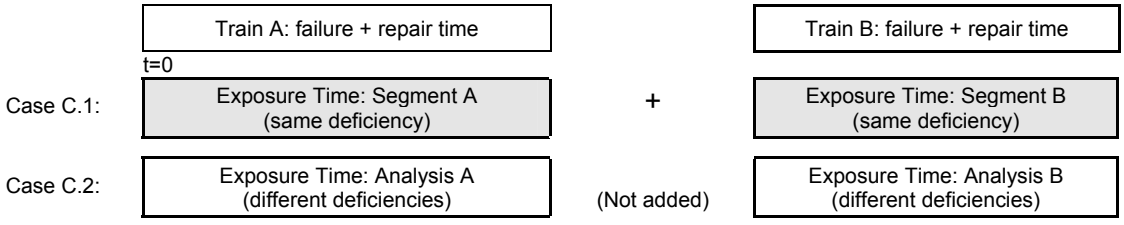
  If both failures were related to the same performance deficiency *(applies to SDP and ASP analyses)* or if both failures are NOT related to the same performance deficiency *(applies to ASP analysis only)*, then the exposure time is the sum of the three segments.



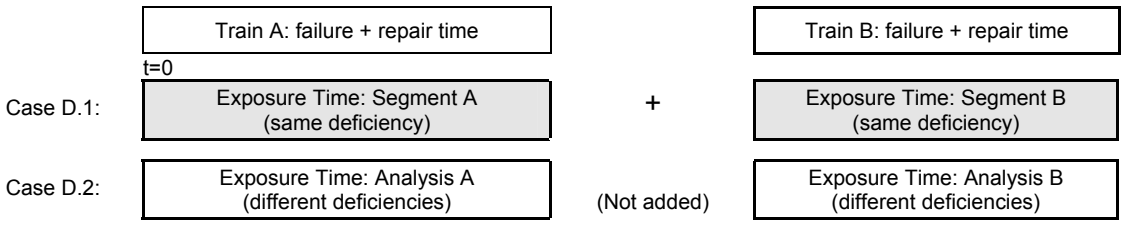
- **Case C - Condition analysis of two failures without overlap.** Failure of one train and a failure in another train with NO overlapping exposure times (same or different systems):

  - Case C.1 - If both failures were related to the same performance deficiency (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)

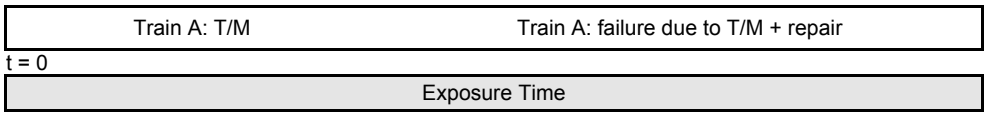
  - Case C.2 - If both failures are NOT related to the same performance deficiency, then each condition is analyzed separately. (Applies to SDP and ASP analyses)



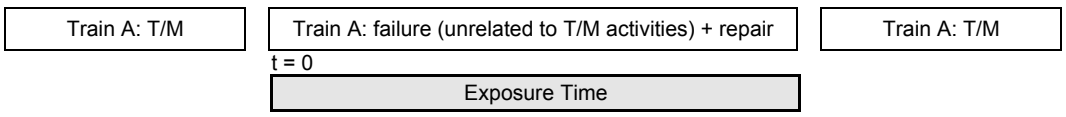
- **Case D - Condition analysis of repeated failures in the same train.**
  - Case D.1 - If both failures were related to the same performance deficiency (other than poor management or cross cutting programs), then the exposure time is the sum of the two segments. (Applies to SDP and ASP analyses)
  - Case D.2 - If both failures are NOT related to the same performance deficiency, then each condition is analyzed separately. (Applies to SDP and ASP analyses)



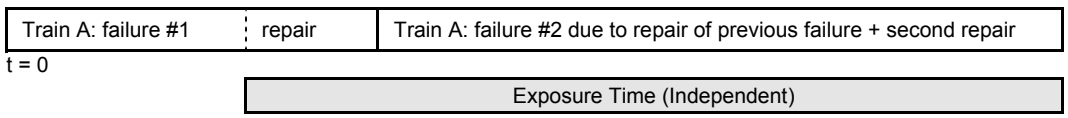
- **Case E - Failure of a train caused by a prior test or maintenance (T/M) activity.**
  - If a component was not properly returned to service following a test or maintenance activity, then the exposure time includes the first maintenance outage time.



- **Case F - Failure of a train NOT caused by test or maintenance (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, latter 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.



3.0 Failure Determination and Modeling

3.1 Types of Failure Modeling

- ***Inoperable.*** A component is “inoperable” if it does not conform to its safety analysis basis. The term "inoperable" has regulatory significance. It does not necessarily imply a state of physical failure. A component can be "inoperable" and still perform its probabilistic risk assessment (PRA) mission.

  For example, vibration in a pump that results in the pump only delivering 500 gpm instead of the rated flow of 600 gpm as required by the Technical Specifications is considered *inoperable*, but 500 gpm is sufficient to meet its function and the pump continued to supply that flow for a period at least equal to the mission time required in the PRA model.

- ***Event severity categories.*** In Section 5.2 of NUREG/CR-6823, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” (Ref. 3-1) component malfunction events are classified into one of the following three *event severity categories*: catastrophic failures, degraded failures, and incipient failures. These categories are summarized 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 non-recovery probability, if applicable, to “True.”

- ***Degraded failures.***

  - *Degraded failures* can prevent a system or train from meeting the success criteria modeled in the PRA model.

  - *Degraded failures* of structures, systems or components (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).

- Setting the basic event to its non-recovery 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 Standardized Plant Analysis Risk (SPAR) model to remove conservatism and thereby reducing the importance of the degradation.

○ Note: Per Supporting Requirement SY-A20 (Capability Category III) in the PRA Standard (Refs. 3-2 and 3-3), 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.

● ***Incipient failures.***

○ *Incipient failures* have no significant degradation in performance but there are indications of a developing fault.

○ 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 open for system operation. 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.***

○ The inability to distinguish between severity levels of failures can be significant especially when dealing with highly reliable SSCs that rarely fail. For a condition analysis, a SSC failure could lead to very high risk. For parameter estimation, the difference between no failures and one failure in estimating the failure rate is much more than the difference between 10 and 11 failures. The analyst should decide whether to call a malfunction a failure or not.

○ Modeling the unknown:

- 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.

3.2 Component Failure Modeling in Event Analysis

- ***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."

- ***Degraded failure without loss of function.***

  - 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 gpm instead of the rated flow of 600 gpm is not a failure event if 500 gpm is sufficient to meet its function and the pump continued to supply that flow for a period at least equal to the mission time required in the PRA model.

  - If the degraded failure was revealed in a short test 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.

- ***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.

  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 Equipment Performance and Information Exchange (EPIX) 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 which can be quickly recovered may be modeled in the PRA as a failure with recovery. Refer to the handbook section on modeling recovery and repair actions in event assessment 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 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 Significance Determination Process (SDP) analyses, the cause of the failures should be related to the same performance deficiency.

  - Refer to the handbook section on exposure time determination and modeling for details and exceptions.

- ***Failure to meet technical specifications.*** An event reported as a failure to meet Technical Specifications, but which would not fail any PRA mission, should not be modeled as a failure. Refer to the above subsection, "Degraded failure without loss of function," for details.

  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. (Note that the 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.) However, this failure would require maintenance to alleviate the fast loading failure.

- ***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 the handbook section on exposure time determination and modeling 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).

3.3 Failure Mode Definitions in SPAR Models

- ***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[3] from Section 5 and Appendix A of NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants" (Refs. 3-6). 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 (Ref. 3-4).

  - 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.

[3] Failure modes used in the SPAR models were identified in the RES system and component reliability studies. See Ref. 3-4 for details. Data used to estimate failure probabilities are primarily from EPIX failure reports. The results were estimated using the RADS calculator (Ref. 3-5). Analysis methods are documented in the parameter estimation handbook NUREG/CR-6823 (Ref. 3-1).

- ***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 (0 - 1 hour) and greater than 1 hour (late).

  - The EDG failure to run logic in the SPAR models may use these same two bins. In older SPAR models, the EDG load sequencer and output breakers are included in the data for the first hour (early) of operation as opposed to being included in the failure to start data.

  - Other SSCs with two bins of failure to run modeled in SPAR models typically include:

    - Turbine-driven pumps
    - Positive-displacement pumps
    - Motor-driven pumps – standby components only
    - Engine-driven pumps
    - Diesel-driven pumps
    - Motor-driven compressors – standby components only
    - Heating, ventilation, and air conditioning (HVAC) fans – standby only
    - Chiller units – standby components only
    - Air Handling/Heating Units
    - Gas turbine generators

  - 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.

3.4 Modeling Failures and Degradations in SAPHIRE/GEM

- ***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 of this volume of the handbook for considerations on this topic.

- ***CCF analysis in event assessment.*** This activity involves the treatment of component failures and degradations with and without common-cause 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 assessment.

  - Refer to Step 4 in Appendix A of this volume of the handbook for considerations on this topic.

  - Note: 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 minimum of the component's input probabilities.

  - Note: A future update of this handbook will provide more explicit guidance on CCF analysis in event assessment.

- ***Importance of process flag selection in SAPHIRE Version 7.***

  - Important note: If setting a basic event to "True" or adjusted 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 process rules for the event tree branch basic event should be reviewed and changes made, if necessary, to allow the correct success probabilities to be determined.

  - The SAPHIRE instructions for setting process flags can be found in Section 1, "Process Flags," of Appendix B of this volume of the handbook.

- ***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 change case.

    Important note: The treatment of CCF events associated with the front line safety system component should reflect the CCF potential of the observed failure in the support system. The CCF events associated with the support system, if any, should be mapped into the front line safety system train. However, this mapping can be complex and will require some thought by the analyst.

  - 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 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 (IA) 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 non-recovery probability can be modeled in top events of an event tree.

- ***Whether to set the basic event to 1.0 or "True" in SAPHIRE/GEM (Version 7).***

  - *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 of this volume of the handbook for considerations on this topic.

  - *Setting the basic event to "True" instead of 1.0*. The following adjustments will be performed by SAPHIRE (Version 7) when a basic event is set to "True":

    - The basic event will be removed from the resulting sequence cut sets.

- "Recovery rule" sets will NOT be applied to resulting sequence cut sets containing the event that was set to "True," such as "disallowed maintenance combinations" rule set for test/maintenance (T/M) outages and dependency rule set for human errors, because of the removed basic event from the cut sets. Illogical or mutually exclusive cut sets may be generated. These cut sets may include random failures of the equipment that is supposedly out for T/M.

○ *Setting the basic event to 1.0 instead of "True."* The following adjustments will be performed by SAPHIRE (Version 7) 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.

- "Recovery rule" sets will be applied to the resulting sequence cut sets, such as "disallowed maintenance combinations" rule set for T/M outages and dependency rule set for human errors. "Recovery rules" will "see" the basic event and operate accordingly.

○ Important note: 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. The analyst may also modify recovery rules to produce the correct cut sets.

3.5 References

3-1. U.S. Nuclear Regulatory Commission, "Handbook of Parameter Estimation for Probabilistic Risk Assessment," NUREG/CR-6823, September 2003. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6823/

3-2. American Society of Mechanical Engineers, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME RA-S-2005, 2005.

3-3. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Revision 1, January 2007. http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-200/01-200r1.pdf

3-4. U.S. Nuclear Regulatory Commission, "Reactor Operational Experience Results and Databases," http://nrcoe.inel.gov/results/, July 2009.

3-5. U.S. Nuclear Regulatory Commission, "Reliability and Availability Data System (RADS)," Database Available in CD Format to NRC Staff Only.

3-6. U.S. Nuclear Regulatory Commission, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," NUREG/CR-6928, February 2007. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6928/

4.0 Mission Time Modeling

4.1 Objective

The objective is to address when a component mission time can be decreased or increased from the 24-hour mission time that is typical credited in PRA sequences.

4.2 Background

- ***Definition: Mission time.*** The PRA Standard (Refs. 4-1 and 4-2) defines *mission time* as ". . . the time period that a system or component is required to operate in order to successfully perform its function."

- ***Overview: Modeling mission time in SPAR models and PRAs.*** Standardized Plant Analysis Risk (SPAR) models assumes a 24-hour mission time for all sequences and most structures, systems and components (SSCs). The supporting requirements in the PRA Standard uses a minimum mission time of 24 hours. However, exceptions are permitted for a shorter and longer mission times for certain situations, as discussed below.

4.3 Considerations: Modeling Mission Times

4.3.1 PRA Standard Requirements – Mission Times

- ***Introduction.*** The supporting requirements from the PRA Standard (Refs. 4-1 and 4-2) for specifying an appropriate mission time for the modeled accident sequences, support systems, and intersystem and intrasystem dependencies are provided below. 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 LOCA, low pressure injection is available for 1 hour, after which recirculation is required, the mission time for LPSI may be 1 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-B10). Examples include:

  - actuation logic
  - support systems required for control of components
  - component motive power
  - cooling of components
  - 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-B12)

4.3.2 Mission Times in SPAR Models

- SPAR assumes a 24-hour mission time for all components for success.

- Mission times can be found in the plant-specific SPAR model manual sections on basic event data and fault tree models.

4.3.3 Other Considerations for Mission Times < 24 Hours

- ***Introduction.***

  - When a failure to run basic event has either a high Fussell-Vesely or a high Birnbaum importance measure in the analysis results, it may be appropriate to reduce the mission time. However, there should be a technical basis for changing the mission time.

  - 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 the SPAR model developer 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.

- Supporting requirements from the PRA Standard should be considered (see Section 4.3.1).

- ***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 support the full sequence mission time.

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

  - 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)

  - 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 (RHR) 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.

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

  - In the past, 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 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.

    A better method is to credit convolution in the SBO model. Convolving the failure distributions eliminates the simplifying assumption that all failures happen at time

zero.[4] SPAR models do not generally use 'convolution' although a methodology and associated failure values have been developed. The fundamental method used in SPAR model for the inclusion of convoluted failure values include appending adjustment factors to specific cut sets. Adjustment factors in SPAR model (may be inactive) are provided in time-dependent basic events (e.g., 30 min., 1 hr, 2 hr, . . .24 hr) for EDG FTR and nonrecovery of offsite power.

- Consult the SPAR model developer for activation of these adjustment factors.

- ***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 (TDAFW) operations.

  - Increasing mission time due to implementation of alternative mitigative strategies, e.g., battery life extension.

4.3.4 SPAR Model Modifications

- ***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 of this volume of the handbook for considerations on this topic.

- ***Modifying mission times in SAPHIRE (Version 7).*** Changing the mission time for a failure to run (FTR) parameter in SAPHIRE (Version 7) may result in a global change throughout the model for that component. 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 cases, the change may be applicable to one sequence or cut set. Recovery rules may be used to replace a basic event with the mission time change. Alternate options include: (1) replace the basic event in the fault tree with a modified basic event with the mission time change or (2) remove the template event from the basic event and fill in the basic event parameters.

  - *Making global changes in SAPHIRE (Version 7).* To make a global change in the mission time of a FTR template event, in SAPHIRE (Version 7): select *Modify*, select *Basic Event*, select the *Event* tab in the *Modify Event* window, and enter the value in the *Mission Time* field.

[4] Quantification without convolution typically involves assumptions like: (1) failure-to-run (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 ($1/\lambda$) is well into the 24-hour mission, (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.

- *Modifying cut sets using recovery rules in SAPHIRE (Version 7).* Recovery rule(s) may be developed to replace a basic event in cut sets with a modified basic event with the mission time change. Recovery 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 recovery rules in the base case SPAR model can be found in the SAPHIRE (Version 7) training manual (Ref. 4-3).

- *Modifying the basic event.* Replace the basic event in the fault tree with a modified basic event with the mission time change. However, be aware of impacts to component-related CCF compound events. Otherwise, remove the template event from the basic event and fill in the basic event parameters in the base case model. Be ware of duplicative usage of the modified fault tree.

- ***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).

4.3.5 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 supportive 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 SAPHIRE (Version 7) project recovery 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 (EOPs) 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?

References

4-1. American Society of Mechanical Engineers, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” ASME RA-S-2005, 2005.

4-2. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities,” Revision 1, January 2007. http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-200/01-200r1.pdf

4-3. U.S. Nuclear Regulatory Commission, “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE): Tutorial,” NUREG/CR-6952, Vo. 4, September 2008. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6952/

5.0 Test and Maintenance Outage Modeling

5.1 Objective

- The objective is to address system, train, or component that was observed disabled for a test or maintenance (T/M) activity. A complex set of manual manipulations in SAPHIRE Version 7.27 are required by the analyst for proper removal of illegal T/M combinations in cut sets by recovery rules.

- SAPHIRE Version 8 will provide a simplified treatment of T/M with less work-around actions from the analyst

- Treatment of a system, train, or component in T/M is application specific. Refer to the program-specific procedure for details (i.e., SDP, ASP, MD 8.3).

5.2 Modeling T/M Events in Event Assessment

- When modeling a system, train, or component that was in T/M, the desired treatment of basic events in the SPAR model is as follows:

    - No illogical cut sets with mutually exclusive T/M combinations (e.g., T/M of a component in one system combined with a failure/unavailability of a component in an associated support system.)

    - Project recovery rule removes all T/M pairs disallowed by plant Technical Specifications (e.g., T/M of multiple components in the same system).

    - Adjustment (increase) in the common-cause failure (CCF) probability associated with the component in T/M in a common cause component group (CCCG) size of three or more. No change in CCF probability for CCCG size of two.

5.3 T/M Events in SPAR Models

- ***SPAR naming scheme.*** T/M basic events are noted with "TM" in the event name (e.g., EPS-DGN-TM-1A)

- ***Recovery rules.*** Project recovery rules are used to remove "disallowed maintenance combinations" from the overall cut sets. The project rules are listed in the plant-specific SPAR model manual (Section 8 for boiling-water reactor (BWR) models, Section 9 for pressurized-water reactor (PWR) models).

- ***Basis of T/M event combinations.*** The mutually exclusive T/M event combinations were taken from the licensee's PRA, where available. Otherwise, a generic rule set was applied to the model.

5.4 Modeling T/M in SAPHIRE/GEM (Version 7.27)

- ***Introduction.*** The procedure for modeling a component that was observed in T/M during an initiating event or concurrent condition (a component unavailable due to failure and another component in T/M during a segment of the failure exposure time) requires multiple manual actions by the analyst in SAPHIRE. These changes can not be performed in GEM. The method will require the update of the base case SPAR model to reflect the T/M unavailability and any other unavailability being modeled in the analysis.

  The modified base case that reflects the elimination of illegal T/M combinations and the increase in core damage probability (CDP) associated with event-specific conditions (e.g., failure of other components) must be subtracted from the CDP of the unmodified base case SPAR model to get the condition importance (ΔCDP). The conditional core damage probability (CCDP) of an initiating event is easier to obtain since no subtraction will be required. The model solutions will not be exact, but should be close in most cases. Nevertheless, the analyst should inspect cut sets for illogical combinations.

- ***Procedure (SAPHIRE Version 7.27).*** When modeling a component that was in T/M, the treatment of basic events in the SPAR model for any CCCG size is as follows:

  - Document the CDF of the baseline SPAR model ("out-of-the-box" base case SPAR model). This will be needed in the last step of this procedure to calculate the final ΔCDP of the condition analysis.

  - Create a *change set* [5] (A):

    - Set the T/M basic event to 1.0 (not "True"). This will ensure that important cut set combinations are not truncated and that the rule processor can remove the T/M combinations disallowed by plant Technical Specifications.[6]

    - For CCCG size of three or more: Set all remaining basic events associated with the component's other failure modes (e.g., FTS, FTR) to "1.0" (not "True").

    - For CCCG size of two: Set the CCF events (e.g., CCF-FTS, CCF-FTR) to "False" to prevent double counting the CCF contribution, since SAPHIRE uses Q_t rather than Q_1 for the independent failure probability.

  - *Generate* [7] change set A.

[5] **Change Sets** are a user-defined set of changes (think data filter) that will be applied (on the base case data) when data is transferred to the current case via the **Generate** option. Multiple change sets can be defined and applied singly or in combination.

[6] SAPHIRE uses recovery rules remove cut sets that contain combinations of equipment in T/M that are not allowed by Technical Specifications. Setting a T/M event to "True" will prevent the event from reaching the cut sets, but will also prevent the correct application these recovery rules. Setting a T/M event to fail by setting the failure probability to 1.0 will result in illogical cut sets. These cut sets will include random failures of the equipment that is out for T/M.

[7] The **Generate** option transfers base case data to the current case (after making changes specified in any marked change sets). SAPHIRE *always* uses current case data for analysis. If the base case data is changed and the **Generate** option is *not* performed, the data that is used for the analysis may not reflect the changes. After changing

- "Solve" all sequences (from top menu select "Sequence," select "Apply Masks," right click select "Solve").

- Create a second change set (B) for modeling the condition or initiating event:

  - Set the T/M basic event to "True". Note that the resulting cut sets may not be in minimal form, since they may include FTS and FTR events of the component in T/M.

  - For a condition analysis, set failed component(s) that is associated with the condition to "True." This assumes the potential for CCF in remaining components in the common-cause component group.

  - For an initiating event analysis, set the components and human actions that were observed to be failed to "True" or those that were degraded to representative failure probabilities. Set the initiator frequency to 1.0 and the other non-initiator frequencies to 0.0.

- *Generate* change set B.

- *Update*[8] cut sets in all sequences (from top menu: select "Sequence," select "Apply Masks," right click select "Cut Sets" and "Update").

- Inspect top cut sets and remove remaining illogical and disallowed cut sets:

  - Inspect cut sets using the list in the next section as a guide (from top menu: select "Sequence," select "Apply Masks," right click select "Cut Sets" and "Update").

  - Check for disallowed cut sets associated with support components that may or may not be modeled with their own T/M events.

  - Remove unwanted cut sets using recovery rules.

- Calculate the importance of the condition without the component in T/M using a new ("out-of-the-box") base case SPAR model.

  - Note: A new base case model is required because the previous "modified" base case model was updated with T/M and failure events set to "True."

  - Use an adjusted condition exposure time without the T/M unavailability time segment.

  - GEM can be used for this analysis.

---

basic event data (in the Base Case, Change Set, or Flag Set), performing the **Generate** option ensures the current case data reflects these changes.

[8] Base case data and results are changed by **updating** the base case. Updating the base case transfers the current case data or results into the base case.

- The final model solution will represent the CCDP of the condition (or initiating event) with a component in T/M.

  - *Condition analysis.* The ΔCDP for a condition analysis with a component in T/M for time (*t)* during the condition exposure time *(ET)* can be calculated from the following approximate equation:

    $$\Delta CDP_{Final} \approx (CCDP_{T/M\ \&\ Condition} - CDP_{Baseline})(t/365) + \Delta CDP_{Condition\ Only}$$

    where:

    $CCDP_{T/M\ \&\ Condition}$ is the result from the above final model solution with the concurrent component availabilities.

    $CDP_{Baseline}$ is the baseline CDP from the "out-of-the-box" base case SPAR model.

    (t/365) is the fraction of time that the component was in T/M (t is duration, in days)

    $\Delta CDP_{Condition\ Only}$ is the importance of only the condition without the T/M unavailability during an exposure time without the T/M unavailability time period.

  - *Initiating event analysis.* The CCDP of an initiating event with a concurrent component in T/M is simply the results of the above final model solution.

5.5 Inspection of Cut Sets

- ***How to check.*** How to check for illogical, and missing cut sets:

  - Check the basic event listing at the end of the GEM report to identify basic events which should have been removed.

  - Inspect cut sets within SAPHIRE (from top menu: select "Sequence," select "Apply Masks," and select "Display" and then "Cut Sets").

  - Review cut sets that contribute to the 95^{th} or 99^{th} percentile of the risk contribution.

- ***What to consider.*** What to consider when reviewing illogical, and missing cut sets:

  - *Illogical cut sets.* T/M combinations not specifically disallowed by Technical Specifications or plant procedures, but are mutually exclusive.

    Examples of possible illogical cut sets include:

    - T/M and a failure (fail-to-start, fail-to-run) of a component in the same system train.
    - T/M of multiple components in the same system.
    - T/M of multiple components in the same division.
    - T/M and a failure of a support system train that supports the division.

- *Disallowed cut sets.* T/M pairs not permitted by Technical Specifications or plant procedures.

  Examples of potential disallowed cut sets (plant-specific) include:

  - T/M of multiple trains in the same system.
  - T/M of both an EDG and turbine-driven auxiliary feedwater pump.
  - T/M of both a support system train (EDG, service water, electrical bus) and equipment in the other division of a frontline system.

This page intentionally left blank

Methods Guide Modeling Recovery and Repair Actions in Event Assessment	Section 6
	Rev. 1.03

6.0 Modeling Recovery and Repair Actions in Event Assessment

6.1 Objective and Scope

The objective is to address what recovery and repair actions can be credited in the risk analysis of an operational event 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.

Guidance in this section is intended for modeling recovery and repair actions in event assessment. Although this guidance can be used to model recovery actions in the base case model, other guides related to building PRA models (Ref. 6-1 through 6-7) 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," (Ref. 6-1) and the PRA Standard (Refs. 6-2 and 6-3). Examples are from NUREG/CR-6823.

  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 *recovery* 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 HVAC system fails, recovering grid-related losses of offsite power by rerouting power, manually initiating a system when the automatic actuation signal fails, bypassing trip logic using jumper cables, and using a hand wheel to manually open an MOV 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*** *(Ref. 6-1).* PRA models typically include 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 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 actuarial 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 can not 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.

References and guides for modeling recovery actions in PRAs are provide in Refs. 6-1 through 6-7.

- ***Overview: Modeling recovery and repair actions in event assessment.*** 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 mitigating strategy. In an event analysis 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, where as 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 Considerations: Modeling Recovery and Repair Actions[9]

- ***Contents***

6.3.1 Considerations: Standard, Regulatory Guide, and NUREGs

- ***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 (Refs. 6-2 and 6-3). 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 recovery and repair actions, including associated index numbers, are provided in Attachment 6-1 to this section.
  - An overview of applicable supporting requirements in Attachment 6-1 include the following considerations:

[9] The terms "recovery", "repair", "recovery event", and "non-recovery" 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. "Non-recovery" 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.

- 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-C1).

○ Additional supporting requirements apply to the modeling of data-based "nominal" repair failure probabilities in the base case PRA. NUREG/CR-6823 (Ref. 6-1) provides guidance for allocating repair and recovery data.

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

- ***Using data to estimate non-recovery probabilities.*** "Nominal" failure probability for a *repair* action is normally based on the evaluation of industry-wide operating experience data. Examples of data-based non-recovery probabilities used in SPAR models include recovery/repair of emergency diesel generator failures and loss of offsite power events.

  ○ Guidance on the process for collecting and reducing recovery and repair data is provided in Section 5.3 of NUREG/CR-6823 (Ref. 6-1). This guidance includes a description of the type of data that is reviewed and guidelines for allocating data.

  ○ Analysts specializing in parameter data collection, reduction, and statistical analysis should be consulted for estimating a non-recovery probability using operational experience data.

- ***Using HRA to estimate non-recovery probabilities (good practices for implementing HRA)***. Failure probability for a *recovery* action is normally derived in an HRA. Good practices from NUREG-1792, "Good Practices for Implementing Human Reliability Analysis," (Ref. 6-4) for crediting post-initiator recovery actions while implementing Regulatory Guide 1.200 (Ref. 6-2) and the related requirements of the ASME Standard (Ref. 6-3) 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 2 of Attachment 6-2 at the end of this section.

  ○ *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. 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 Attachment 6-1to this section and in Section 6.3.2 below.

- Good Practice #3*: Quantify the Probability of Failing to Perform the Recovery (ies).* Quantify the probability of failing to perform the recovery(ies) 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):

  - Sect. 5.1, "Identifying Potential Post-Initiator HFEs"
  - Sect. 5.2, "Modeling Specific HFEs Corresponding to Human Actions"
  - Sect. 5.3, "Quantifying the Corresponding HEPs for Post-Initiator HFEs"

6.3.2 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 Attachment 6-2 to this section. These questions were developed largely from the PRA Standard (Ref. 6-3), NUREG-1792 (Ref. 6-4), 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 2 of Attachment 6-2 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 considered in the HRA (and in the recovery/repair plausibility and feasibility determination). This is consistent with the *failure memory*[10] approach.

- 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 failure 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 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.

- ***Examples of failure events and associated potential recovery actions.*** The below table provides examples of failure events and associated potential recovery actions.

Examples of Initial Failure Event(s)	Potential Recovery/Repair Action
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 Technical Specification inoperable for the test/maintenance but can be returned to service quickly)
Failure on demand (electrical, e.g. fuse or other electrical fault which can be recovered)	Replace fuse or if a control power problem, locally manually shut the breaker
Failure on demand (mechanical)	Use redundant SSC or a functionally similar component; 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

[10] The "failure memory" approach is used to estimate the risk significance of operational events. In a 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.

- ***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 in parts on the floor. 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 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 to recovery. Therefore, the recovery credit would be assigned to the EDG that can be restored to service earlier.

  - *Recovery/repair of failures in two systems* may be a burden on plant staff, except when ample time 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 (HPI) systems may be difficult within the short time available, whereas, recovery of AFW and residual heat removal (RHR) 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.

    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 recovery should be based on more pessimistic characteristics (e.g., less time available, less resources) than if such a possibility is not considered.

- ***Consideration of dependencies among multiple human actions in a cut set***. Particular attention should be paid to accounting for dependencies among the human failure events (HFEs) including the credited recovery/repair actions. Considerations from NUREG-1792 (Ref. 6-4) 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 (PORV) path remained open in the Three Mile Island accident, despite new cues of the problem, different personnel arriving, etc.

- Assessing no dependence needs to be adequately justified and documented to ensure that credit for the recovery action(s) is not unduly optimistic.

- ***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 (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 auxiliary feedwater (TDAFW) pump after 2 hours following a station blackout can result in doubling the time to core uncovery.

  Some considerations when crediting recovery/repair from a failure to run (FTR) event:

  - *Increase in "time available" for diagnosis and operator actions.* Extended time may increase the "time available" performance shaping factor in the human reliability analysis of diagnosis and operator actions in some sequences as well as 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.

6.3.3 SPAR Model Modifications

- ***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 "recovery rule" (discussed further in this section) 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. Consideration for adding a recovery event at the various levels in the SPAR model include:

- *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, "recovery rules" may be needed to apply a time-dependent recovery action (e.g., EDG non-recovery 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, "recovery 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."[11]

  - Important Note: See the considerations in "Using an existing recovery event in the SPAR model" in Section 6.3.3 when reusing existing basic events and "recovery rules."

  - 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. "Recovery 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 applicable cut sets must be identified before the "recovery rules" can be written. Considerations include:

  - To unsure 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." Setting probability to "1," 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.

[11] 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.

- Look for dependencies (e.g., recovery/repair time, HEP) between the recovery event(s) and other events in the cut sets.

- Write "recovery 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 CDF, thus increasing 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 an event assessment, 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 "nominal" non-recovery 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 "nominal" non-recovery 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 non-recovery 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 "nominal" non-recovery probability is already included in the base case model (e.g., EDG repair), then either

      (1) 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

(2) 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 alternative mitigating strategies*. As a general rule, an alternative mitigating strategy should be credited 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.

- Important Note: See the considerations below for using existing SPAR model basic events. Otherwise, create new basic events.

- ***Consult the SPAR model developer.*** Changes to the SPAR model should be closely coordinated with the SPAR model developer to ensure changes are completely reflected throughout the model. Review checklists for SPAR model modifications are provided in Volume 3 of this handbook.

- ***Using an existing recovery event in the SPAR model***. The base case SPAR model contains few recovery events that include basic events and "recovery rules" with nominal failure to recover probabilities (e.g., EDG, loss of offsite power). 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 "recovery 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., CCF)
    - Template event shared by basic events of a component group (e.g., motor-driven pump, motor-operated valve)
    - Basic event used in "recovery rules"

  - Examples of basic event parameter variables that could impact multiple parts of the model include:

- Failure probability/rate
- Mission time
- Calculation type
- 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 "recovery rules."*** "Recovery rules"[12] are free-form logic rules that allow for the alteration or deletion of fault tree or sequence cut sets in a "post-processing" fashion. "Recovery 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 "recovery 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.

  ○ "Recovery 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)

    List of each type of "recovery rule" can be viewed from 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. Since the component event is set to "True," a subtree will be needed to model the recovery and operation of the component during restart and throughout the remainder of its mission time. (See example, below).

  ○ *Use the correct fault tree logic (an example).* An example of subtree logic for a repair model that can be added to an existing fault tree is shown in the figure below. Elements of the subtree example are summarized below.

    - A new recovery event (Operator Fails to Repair MDP-3A) is created and the failure probability is set to the HRA-derived estimate (HEP = 0.1) in

[12] Although called "recovery rules," 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.

the change case to represent observed failure and cut set dependences. If HEPs are cut set dependent, then "recovery 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 subtree 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 common-cause failure (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" base case model.

- The CCF subtree is slightly different than the independent failure subtree 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 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 subtree (Operator Fails to Repair MDP-3A) is the same basic event used in the independent failure subtree. 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 (Ref. 6-1) 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).

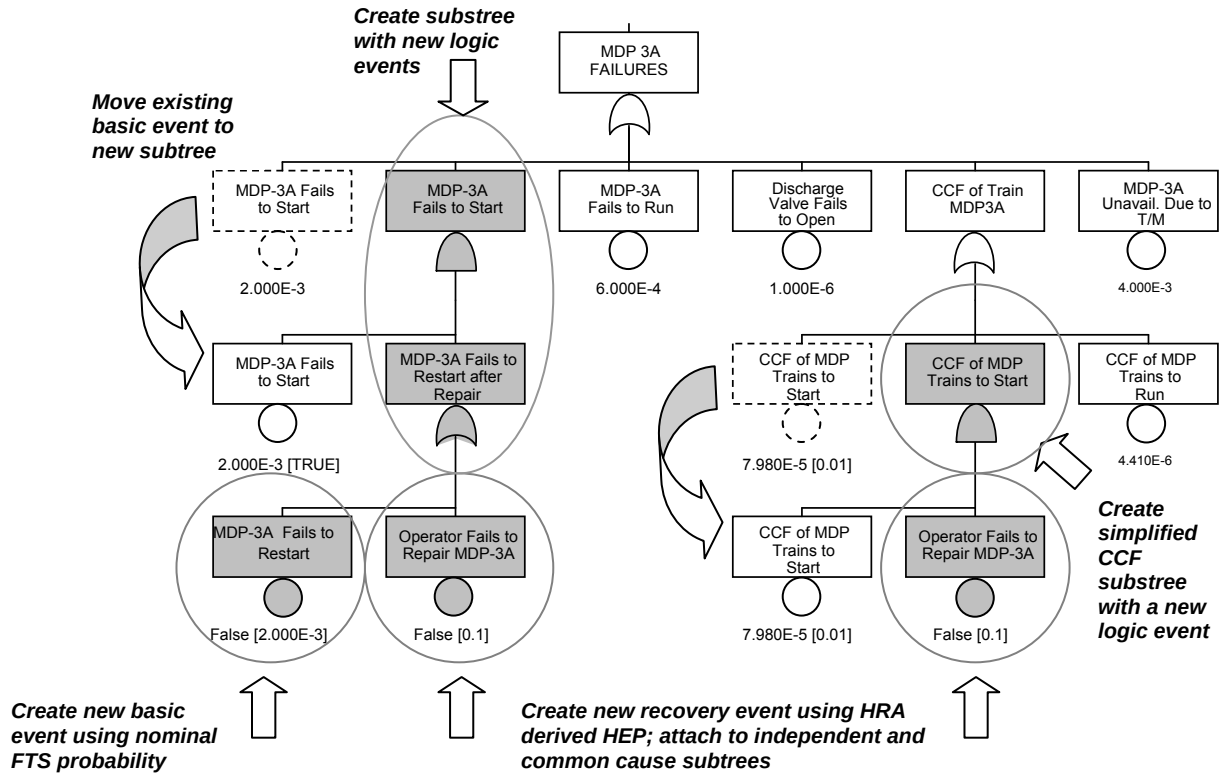


Figure 6-1. An example of subtree logic for a repair model added to an existing fault tree. (The basic events in the figure show example base case and change set values).

- *Select the Process Flag.* When modifying a fault tree that results in a high failure probability (e.g., 0.1 to 1.0), set the appropriate process flag. This is especially important for top events with a single basic event for the fault tree.
  - The SAPHIRE instructions for setting process flags can be found in Appendix B of this handbook volume.
- *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 core damage frequency (CDF) of the base case SPAR model.
  - For repair actions, the recovery event in the base case model should be set to "False" or "True" (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.

6.4 References

6-1. U.S. Nuclear Regulatory Commission, "Handbook of Parameter Estimation for Probabilistic Risk Assessment," NUREG/CR-6823, September 2003. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6823/

6-2 U.S. Nuclear Regulatory Commission, Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Revision 1, January 2007. http://www.nrc.gov/reading-rm/doc-collections/reg-guides/power-reactors/active/01-200/01-200r1.pdf

6-3 American Society of Mechanical Engineers, "Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications," ASME RA-S-2005, 2005.[13]

6-4 U.S. Nuclear Regulatory Commission, "Good Practices for Implementing Human Reliability Analysis (HRA)," NUREG-1792, April 2005. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1792/

6-5 U.S. Nuclear Regulatory Commission, "PRA Review Manual," NUREG/CR-3485, September 1985.

6-6 U.S. Nuclear Regulatory Commission, "Interim Reliability Evaluation Program Procedures Guide," NUREG-2728, January 1983.

6-7 U.S. Nuclear Regulatory Commission, "A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants," NUREG/CR-2300, January 1983. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr2300/

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

This page intentionally left blank

Attachment 6-1: PRA Standard Supporting Requirements

The supporting requirements to the PRA Standard (Refs. 6-2 and 6-3) for crediting and modeling recovery and repair actions, including associated index numbers, are provided in this attachment. For the most part, these supporting requirements can be used to model recovery and repair actions in an event assessment. Questions regarding interpretations and clarifications should be directed to a 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.

Note: Clarifications to the ASME Standard in the Regulatory Guide 1.200 are emphasized in bold italics below.

PRA Standard Supporting Requirements for Modeling Recovery in PRAs

- **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.

  Note: 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 human reliability analysis (HRA) (i.e., PRA Standard designators HR-E through HR-G). They are included to allow credit for recovery form 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**.

- **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:

  (a) A procedure is available and operator training has included the action as part of crew's training, or justification for the omission is provided.

  (b) "Cues" (e.g., alarms) that alert the operator to the recovery action provided procedure, training, or skill of the craft exist.

  (c) Attention is given to the relevant plant-specific and scenario-specific performance shaping factors provided in **HR-G3** as follows:

  (d) There is sufficient manpower to perform the action.

- **HR-H3:** Account for any dependency between the human failure event (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 performance shaping factors:

  (a) Quality [type (classroom or simulator) and frequency] of the operator training or experience
  (b) Quality of the written procedures and administrative controls
  (c) Availability of instrumentation needed to take corrective actions
  (d) Degree of clarity ***of the meaning*** of the cues/indications
  (e) Human-machine interface
  (f) Time available and time required to complete the response
  (g) Complexity of ***detection, diagnosis and decision-making, and executing*** the required response
  (h) Environment (e.g., lighting, heat, radiation) under which the operator is working
  (i) Accessibility of the equipment requiring manipulation
  (j) 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. Account for the influence of success or failure in preceding human actions and system performance on the human event under consideration including

  (a) Time required to complete all actions in relation to the time available to perform the actions
  (b) Factors that could lead to dependence (e.g., common instrumentation, common procedures, increased stress, etc.)
  (c) Availability of resources (e.g., personnel)

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

- **SY-A22:** 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 DA-C14 and estimated in accordance with DA-D8.***

- **DA-C14:** For each structure, system and component (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-D8,*** 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-D8:** For each SSC for which repair is to be modeled, estimate, based on the data collected in DA-C14, 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 requantifying 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.

Attachment 6-2: Questions to Consider for Crediting Recovery or 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.

1.0 Questions to Consider During the Event Investigation

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?

2.0 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:

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

- o Time to core uncovery
- o Time to recover vessel water level before pressure exceeds pump injection limits (low pressure - pump runout; high pressure - pump shutoff head)
- o Time to suppression pool overpressure failure
- o Time to suppression pool temperature exceeding net positive suction head (NPSH) limits

☐ Can the recovery/repair action be accomplished within the required time frame? Considerations include:

- o Tools readily available
- o Spare parts readily available
- o Area lighting and power sources for tools available
- o Communications with control room available
- o Plant staffing level with the right skills

Note: Full plant staffing available would be about 25% of the year during power operations. However, the emergency response organization should be activated within 2 hours following the scenario initiation.

☐ 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 the quality and frequency of the training is adequate?

☐ Is there procedure guidance to perform the recovery (ies)?

☐ Are the equipment needed to perform the recovery (ies) 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?

7.0 Multi-Unit Considerations Modeling

7.1 Introduction

- ***Overview.*** 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 diesel generators
    - Alternate 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 subtree 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 (CCF) 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 (LOCAs)), 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 & 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 station blackout 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 performing shaping factors in accordance with the human reliability analysis methodology.

7.3 Examples

The following ASP analysis can be viewed from the ASP database (Ref. 7-1).

- Final ASP Analysis for LER 266/01-005, " Point Beach 1 and 2 Potential Common Mode Failure of All Auxiliary Feedwater Pumps," event date November 29, 2001.

- Final ASP Analysis for LER 280/01001, "Surry Units 1 & 2 Diesel Generator #3 Inoperability Caused by Insufficient Lubricant," event date April 23, 2001.

- Final ASP Analysis for LER 316/01-003-01 and Inspection Report Nos. 50-315/01-17, 50-315/01-19, 50-316/01-17, & 50-316/01-19, "D. C. Cook Units 1 & 2 Degraded ESW Flow Renders Both Unit 2 Emergency Diesel Generators Inoperable, and Turbine Driven AFW Failed Due to Insufficient Engagement of the Trip Latch Mechanism for the Turbine Trip Throttle Valve," event dates August 9 and 29, 2001.

7.4 Other Suggested Readings

- S.E. Mays, et al., "Multi-Unit IPE and PRA Issues," Proceedings of the International Topical Meeting on Probability, Reliability, and Safety Assessment PSA '89, Pittsburgh, PA, 1989.

- Woo Sik Jung, et al., "A New Method to Evaluate Alternate AC Power Source Effects in Multi-Unit Nuclear Power Plants," Reliability Engineering and System Safety, Vol. 82, pp. 165-172, 2003.

7.5 References

7-1. U.S. Nuclear Regulatory Commission, "Accident Sequence Precursor Database," https://nrcoe.inel.gov/secure/aspdb/, August 2007. *(NRC internal Web site - available to NRC staff only)*

Appendix A – Road Map: Risk Analysis of Operational Events

Contents

- Modeling degraded structures, systems, and components
- Modeling success
- Common-cause failure analysis in event assessment
- Modeling human errors
- Modeling unavailability due to test or maintenance
- Modeling exposure time (condition duration)

Step-5: Estimation of Event Significance (Initial Model Solution)

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

Step-6: Review of Initial Model Solution Results

- Documentation
- Change case inputs
- Condition exposure time
- Truncation value
- Cut sets
- Multiple operator actions
- Importance measures
- Model uncertainties
- Reasonableness review

Step-7: Recovery Analysis and Model Solution

Step-8: Review of Final Analysis Results

- Inputs and assumptions
- Plant design and operations (as-built, as-operated)
- Documentation
- Sequences and cut sets
- Results

Step-9: Sensitivity and Uncertainty Analyses

- Key SPAR model assumptions and technical issues
- Sensitivity analysis
- Uncertainty analysis

Step-10: Analysis Documentation

References

Acronyms

ΔCDP	increase in core damage probability
ASP	accident sequence precursor
BWR	boiling water reactor
CCDP	conditional core damage probability
CDP	core damage probability
CCCG	common cause component group
CCF	common-cause failure
EPIX	Equipment Performance and Information Exchange
HEP	human error probability
LER	licensee event report
LOCA	loss-of-coolant accident
LOOP	loss of offsite power
NPRDS	Nuclear Plant Reliability Data System
PSF	performance shaping factor
PRA	probabilistic risk assessment
PWR	pressurized water reactor
RADS	Reliability and Availability Data System
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SDP	Significance Determination Process
SPAR (model)	Standardized Plant Analysis Risk model
SSC	structure, system, and/or component
T/M	test or maintenance

Introduction

The following road map describes 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.

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 term "event," when used, refers to either an initiating event or a degraded condition.

Overview

Process overview. The overall event analysis process involves the modification of a 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) Phase 3, NRC Incident Investigation Program [Management Directive (MD) 8.3], and Accident Sequence Precursor (ASP) 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.[14] 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.

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.

[14] 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. A component that has been declared inoperable based on Technical Specifications may be functional (and therefore not failed) from a risk standpoint.

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 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." 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.

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 a topic for a future volume in this handbook.

Overview of this Road Map

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

Sections 2 through 7 in the main body of this handbook (Volume 1) provide additional guides that detail acceptable methods and approaches that have been applied, reviewed, and approved in past ASP and SDP Phase 3 analyses. The tasks in the following road map will refer to these method-specific guides.

Iterative nature of analyses. As shown in Figure 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 PRA model that best represents the as-built, as-operated plant and the operational event.

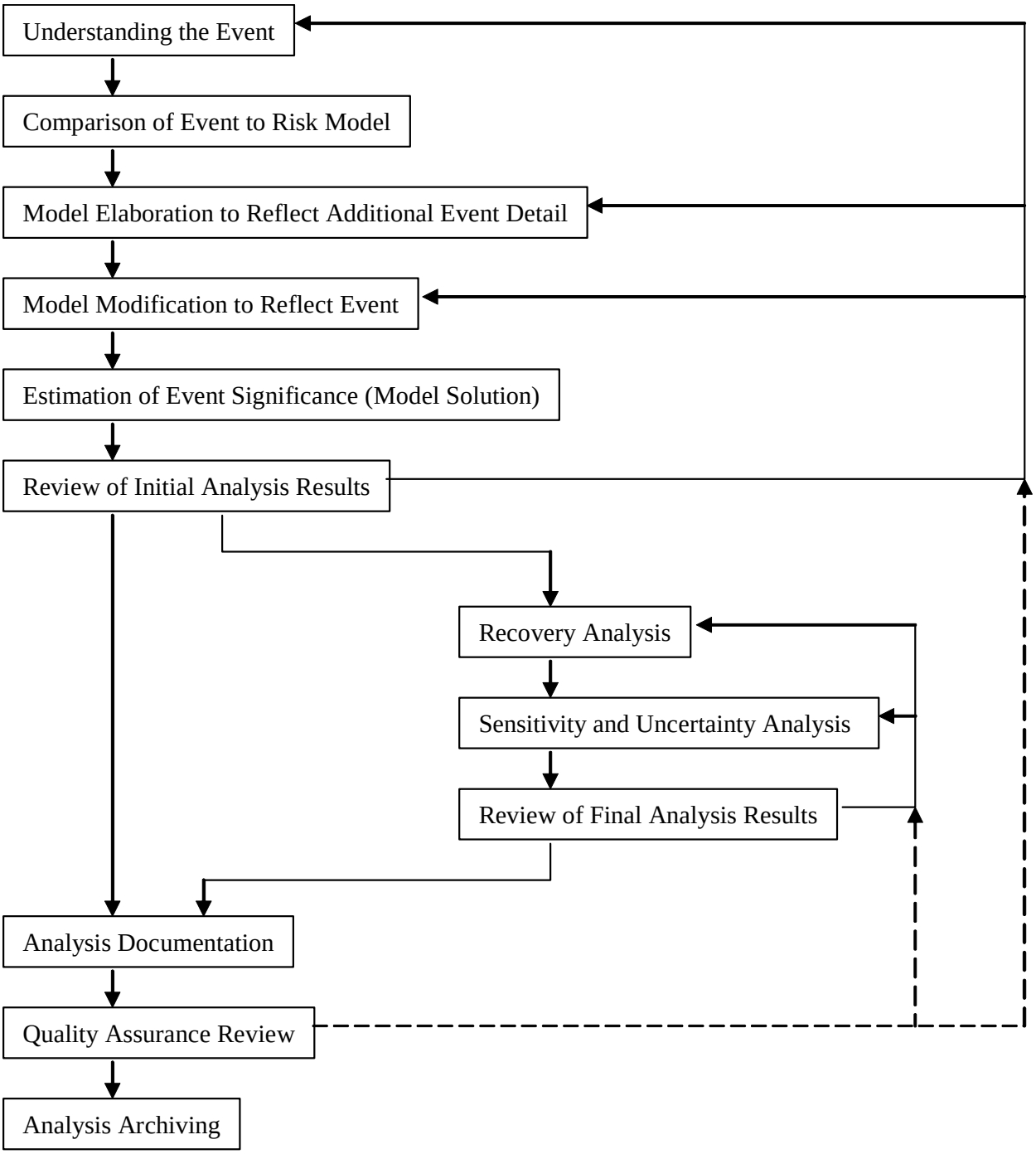


Figure 1. Risk Analysis of Operational Events - Process Flow

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.

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.

☐ All factual information should refer to a traceable reference, such as root cause analyses, inspection reports, plant drawings, system descriptions, procedures, and discussions with NRC and plant staff.

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 which 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 initiating event and condition analysis.

☐ 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, 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 to initiating event analysis.

☐ 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 to condition analysis.

☐ 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, MD 8.3). Licensee event reports (LERs) issued at least one year before the first condition should be reviewed for other overlapping unavailable components.

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 the RASP handbook. Refer to the handbook sections in Volume 2 on modeling considerations for the following operational events:

- Internal fire events (conditions and initiating events)
- Internal flooding events (conditions and initiating events)
- Seismic events (conditions and initiating events)
- Severe weather events (conditions and initiating events)

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, "As-Built, As-Operated Plant Description Review Checklist," 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, "SPAR Model Assumptions and Technical Issues Review Checklist," 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 to the SPAR model developers at the Idaho National Laboratory. Use the feed back form from the SAPHIRE User Group Web site (Ref. 11).

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. This step may include the following activities:

- Event tree modification
- Fault tree modification
- Initiating event frequency parameter update
- Basic event parameter update - component failure probability or rate
- Basic event parameter update - common-cause failure probability
- Basic event parameter update - human error probability
- Solving and saving the modified model

Some considerations include the following:

☐ ***Check SPAR model assumptions.*** Review the SPAR model assumptions (e.g., event tree, fault tree, parameter basis) in the plant SPAR model manual before making changes.

☐ ***Event tree modification.*** 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
  - Changes to an *event tree linking rule*[15] that replace the default fault tree with a substitute fault tree
  - 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 (Refs. 1, 2, and 3).
- A checklist for aiding in the review of event tree modifications is provided in Volume 3 of this handbook.

☐ ***Fault tree modification.*** 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:

[15] *Event tree linking rule* - 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. A rule editor is in SAPHIRE.

- 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 common-cause failures 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 the SPAR model developer.
- SAPHIRE instructions for creating and modifying faults trees in the SPAR model are provided in the SAPHIRE training manuals (Refs. 1, 2, and 3).
- A checklist for aiding in the review of fault tree modifications is provided in Volume 3 of this handbook.

☐ ***Initiating event frequency parameter update.*** 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 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 AC bus. (Note: a nominal initiating event frequency will be estimated and assigned for the modified base case SPAR model.)

- 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, “Handbook of Parameter Estimation for Probabilistic Risk Assessment” (Ref. 4).

    - Initiating event frequencies used in SPAR models are typically based on the analysis methods and results[16] from Section 8 and Appendix D of NUREG/CR-6928, “Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants” (Ref. 5). Updates will be posted on the “Reactor Operational Experience Results and Databases,” Web page.

[16] 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 RADS calculator. Analysis methods are documented in the parameter estimation handbook NUREG/CR 6823 (Ref. 4).

- 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-4550, NUREG/CR-5750).

- 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 (Refs. 1, 2, and 3).

- 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.*** 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 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.

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

  - Basic event used in different fault trees.
  - Basic event used in a compound event (e.g., CCF event)
  - Template event shared by basic events of a component group.
  - Basic event used in recovery 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, "Handbook of Parameter Estimation for Probabilistic Risk Assessment" (Ref. 4).

    - Failure probabilities used in SPAR models are based on the analysis methods and results[17] from Section 5 and Appendix A of NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants" (Ref. 5). 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 Individual Plant Examination (IPE), or generic estimates from legacy sources (e.g., NUREG/CR-4550).

  - Refer to the plant SPAR model manual for the basis for parameter estimates.

[17] Data used to estimate failure probabilities are primarily from Equipment Performance and Information Exchange (EPIX) failure reports. The results were estimated using the RADS calculator. Analysis methods are documented in the parameter estimation handbook NUREG/CR 6823.

- SAPHIRE instructions for creating and modifying basic event parameters in the SPAR model are provided in the SAPHIRE training manuals (Refs. 1, 2, and 3).

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

☐ ***Basic event parameter update - common-cause failure probability.*** This activity involves the update, modification, or creation of a common-cause failure (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.

- Common-cause failure probabilities used in SPAR models are based "CCF Parameter Estimations, 2005 Update" or recent report (Ref. 6).

- The data collection and analysis methods[18] used to update CCF parameters in Ref. 6 are based on NUREG/CR-6268, "Common-Cause Failure Database and Analysis System: Event Collection, Classification, and Coding." (Ref. 7)

- 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. 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 Ref. 6 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 (Refs. 1, 2, and 3).

- 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.*** This activity involves the modification or creation of a human error probability (HEP) 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 task.

Some considerations for parameter modifications include the following:

- Reasons to change or create a HEP basic event parameter in the base case SPAR model may include:

  - Create a new HEP basic event parameter in an event tree or fault tree that represents

    - Non-recovery (diagnosis and action) of the failed/degraded component or system,

    - Human failure (diagnosis and/or action) that was observed to during the operational event,

    - Deficiency in an operating procedure, or

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

  - 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 an HEP parameter performance shaping factor (PSF) that represents a unique plant-specific design feature makes the use of the generic SPAR model 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 test or maintenance, 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 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., PWR, BWR) 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 used in the SPAR model[19] are provided in the table notes in Appendix E of the plant SPAR model manual.

  - 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 based on NUREG/CR-6883, “The SPAR-H Human Reliability Analysis Method” (Ref. 8).

[19] Most HEPs in the SPAR model were estimated using the SPAR-H HRA 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 “True” value.

- The human reliability analysis worksheet for each HEP that was estimated using the SPAR-H HRA 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" (Ref. 9). Refer to Section 3.8 (p. 3-136) and Table 4.1 (p. 4-9) for evaluation of the SPAR-H method.

- "Good practices" for performing HRAs and reviewing HRAs to assess the quality of those analyses are documented in NUREG-1792, "Good Practices for Implementing Human Reliability Analysis" (Ref. 10). Good practices[20] 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.

- SAPHIRE instructions for creating and modifying basic event parameters in the SPAR model are provided in the SAPHIRE training manuals (Refs. 1, 2, and 3).

- 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.

- *Truncation input.* Solve the modified base case SPAR model using the same truncation probability as the original base case SPAR model.

- *Cut set reviews.* 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.

[20] "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 (RG) 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.

- 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 through 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. Recovery rules may be applied to eliminate the unwanted combinations.

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

- *Importance measures review.* Using the risk achievement and risk reduction importance measures, 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.

☐ ***Documentation.*** 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.

☐ ***Report model enhancements to INL.*** Changes to the original base case SPAR model that should be permanently reflected in the master plant SPAR model should be reported to the SPAR model developer at INL. 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 to INL using the "SPAR Model Change Logging System" that can be accessed from the SAPHIRE Users Group Web site (Ref. 11).

Step-4: Create a Change Case to Reflect the Event

In this step, a change case[21] refers to changes to basic event probability data in the base case SPAR model to reflect the failures, unavailabilities and other undesirable occurrences observed

[21] *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

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.

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 non-recovery probability
- Modeling failed structures, systems, and components
- Modeling degraded structures, systems, and components
- Modeling success
- Common-cause failure analysis in event assessment
- Modeling human errors
- Modeling unavailability due to test or maintenance
- Modeling exposure time (condition duration)

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

☐ ***Identify analysis boundary conditions.*** In this activity, the analyst defines the event boundaries in accordance with program-specific procedures (i.e., SDP, ASP, 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 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).

---

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*.

☐ ***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.

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)
  - Basic event used in "recovery rules"
- Examples of basic event parameter variables that could impact multiple parts of the model include:
  - Failure probability/rate
  - Mission time
  - Calculation type
  - 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.*** 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 1.0 to the applicable initiator. Set the initiating event frequencies of non-applicable initiating events to 0.0. GEM performs this setting automatically when the initiator is selected at the beginning of the session.
- 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: $p(\text{initiator}) = 1 - e^{-\lambda \times \text{exposure time}}$. This is approximately ($\lambda \times$ exposure time) for ($\lambda \times$ exposure time) < 0.1. GEM performs this calculation automatically when the exposure time (in hours) is entered into the *Event Duration* window at the end of the condition analysis session.

☐ ***Modeling initiating event recovery actions.*** 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 non-recovery of a system-induced initiator.[22] More than one non-recovery event may be modeled in an event tree, such as early and late recovery actions. The nominal non-recovery 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 of the analysis.

☐ ***Modeling failed structures, systems, and components.***[23] 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, fail-to-run, fail-to-open, fail-to-close).

Some considerations for modeling a failed SSC include the following:

- See the handbook section in Volume 1 on failure determination and modeling 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 fail during the mission (e.g., a pump that fails after running for four hours) a specific reliability analysis is required. See the handbook section in Volume 1 on failure determination and modeling for details.
- Do not credit an observed successful recovery action except probabilistically in a recovery analysis (see Step 7, below).

---

[22] Examples of event trees in SPAR models with non-recovery actions may include loss of offsite power, loss of main feedwater, loss of power conversion system, general transient, loss of instrument air, and loss of service water.

[23] A structure, system, or component 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.

☐ ***Modeling degraded structures, systems, and components.***[24] 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., fail-to-start, fail-to-run, fail-to-open, fail-to-close). 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 <u>not</u> 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 Technical Specifications.
- 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.

[24] 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.

- Document uncertainties associated with the estimate for use in later sensitivity and uncertainty analyses.

- Bounding estimate in an event analysis should not be considered unless the bounding estimate has little impact on the overall analysis results (e.g., bounding analyses can be used in a screening analysis to eliminate an event from further consideration).

- Note: 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 minimum of the component's input probabilities.

☐ ***Modeling success.***[25] 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 0.0. 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:

- Structures, systems and components 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 human error probability equal to the nominal human failure probability.

☐ ***CCF analysis in event assessment.*** This activity involves the treatment of component failures and degradations with and without 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. Future versions of SAPHIRE (Versions 7.28 and 8) will provide advanced capabilities for the analyst, such as exact solutions and complete automation based on a component's state (e.g., failed, degraded, unavailable due to test/maintenance).

Some considerations include the following:

[25] The "failure memory" approach is used to estimate the risk significance of operational events. In a 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.

- *SAPHIRE Version 7.27 instructions.* The CCF probability adjustment will be performed in SAPHIRE Version 7.27 based on multiple inputs from the analyst. These inputs are also based on the analyst judgment that the observed failure has CCF potential or not with other components in the common cause component group.

  For example, the set of instructions for modeling an observed single failure of a basic event that was judged by the analyst to have potential for CCF (Case 1) or no potential for CCF (Case 2) is as follows:

One Component FTS or FTR	CCCG Size 2	CCCG Size 3
CCF Potential (Case 1)	Set basic event for observed failure mode (FTS or FTR) to "True" and Set CCF basic event for unobserved failure mode (CCF-FTS or CCF-FTR) to "False."	Set basic event for observed failure mode (FTS or FTR) to "True" and Set basic event for unobserved failure mode (FTS or FTR) to 1.0.
No CCF Potential (Case 2)	Set basic event for observed failure mode (FTS or FTR) to "True" and Set CCF basic events for **both** failure modes (CCF-FTS **and** CCF-FTR) to "False."	Set basic events for **both** observed and unobserved failure modes (FTS **and** FTR) to 1.0 (not "True"), and Review minimal cut sets to make sure non-minimal cut sets are not significant contributors.

  Refer to the NRC P-501 course manual (Ref. 14) for detailed discussions on how SAPHIRE Version 7.27 adjusts the CCF probability for various cases. Note that these instructions are interim work-around instructions and will be replaced by an exact calculation method in future versions of the SAPHIRE code.

- *SAPHIRE Version 7.28 or 8 instructions.* Refer to the revised SAPHIRE user manual once the new code has been released.

- A future update of this handbook will provide more explicit guidance on CCF analysis in event assessment.

☐ ***Modeling human errors.*** 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 human error probability (HEP) basic events 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 performance shaping factor (PSF) to a higher level.

Some considerations for modeling human errors include the following:

- An observed human error is modeled by setting the appropriate basic event HEP in the SAPHIRE/GEM change case to "True."

- An adjustment to an HEP event based on observed performance deficiencies can be performed using one of the publically available NRC human reliability analysis (HRA) methods, such as

  - The HRA approach use in SPAR models as documented in NUREG/CR-6883, "SPAR-H Human Reliability Analysis Method" (Ref. 8), or

- The second-generation HRA method called "A Technique for Human Event Analysis," (ATHENA), NUREG-1624 (Refs. 12 and 13), 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 HRA method used to quantify an 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.

- Strengths and limitations to the SPAR-H, ATHEANA, and other HRA methods are evaluated in NUREG-1842, "Evaluation of Human Reliability Analysis Methods Against Good Practices" (Ref. 9).

  - *SPAR-H.* Refer to Section 3.8 (p. 3-136) and Table 4.1 (p. 4-9) for the evaluation of the SPAR-H HRA method.

  - ATHEANA. Refer to Section 3.9 (p. 3-150) and Table 4.1 (p. 4-10) for the evaluation of the ATHEANA HRA method.

- "Good practices" for performing HRAs and reviewing HRAs to assess the quality of those analyses are documented in NUREG-1792, "Good Practices for Implementing Human Reliability Analysis" (Ref. 10)[26]. 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.

- Request assistance from a human reliability analyst.

- A future update of this handbook will provide more explicit guidance on HRA in event assessment.

☐ ***Modeling unavailability due to test or maintenance.*** This activity involves the treatment of a system, train, or component that was disabled for T/M activity during the operational event.

Some considerations for modeling components in T/M include the following:

- Refer to the handbook section in Volume 1 on test and maintenance outage modeling for guidance.

[26] "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 (RG) 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.

- The common-cause plug-in modules in SAPHIRE Version 7.27 do not automatically calculate the CCF probability with a component in a common cause component group that was disabled for T/M activity. The analyst must make manual adjustments in SAPHIRE to account for the T/M unavailability. Refer to handbook section in Volume 1 on test and maintenance outage modeling for details.

  Future versions of SAPHIRE (Versions 7.28 and 8) will provide advanced capabilities for the analyst, such as exact solutions and complete automation based on the status of a component (e.g., failed, degraded, unavailable due to test/maintenance).

- Treatment of a component in T/M is application specific. Refer to the appropriate program-specific procedure (i.e., ASP, SDP, 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 Phase 3 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 under assessment.

☐ ***Modeling exposure time (condition duration).*** The exposure time (sometimes known as failure or condition duration) is used by the SAPHIRE/GEM code in a condition analysis to model the duration over which the risk of the condition (i.e., failure, degradation) is measured. After SAPHIRE/GEM 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 the handbook section in Volume 1 on exposure time determination and modeling 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. Refer to the handbook section in Volume 1 on exposure time determination and modeling for additional details.

- 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, 3, and 4, 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
- 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.

- Always review the results. 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 re-solution with a lower truncation value. These cut sets may be truncated out in the base case SPAR model results.

- *Rule of thumb.* Truncation values of 1E-12 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.

Note: Analysis of loss of offsite power initiating events often result in significantly longer runtime than other initiators due to extensive logic associated with emergency diesel generators and their support systems.

- Refer to the plant SPAR model manual, "Notes to Analysts," for additional details on truncation values. In addition, an investigation into the truncation issue conducted by the Idaho National Laboratory is documented in a report entitled, "Truncation Insights."

☐ ***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 frequency of 0.0). Second, set the initiator that *did* occur to "True" (or frequency 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 CCDP. Second, a condition analysis (with the initiating event probabilities remain at the base case or nominal value) should be performed to determine the "importance" 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, 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 increase in core damage probability (ΔCDP) or "importance" 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. The importance result is documented in the GEM printout.

☐ ***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., ASP, SDP, 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 performance deficiency are considered in one analysis; otherwise, each performance deficiency is treated in a separate SDP analysis.

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

- Refer to the table in the handbook section on exposure time determination and modeling for examples of exposure time modeling of concurrent 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
- 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:

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

☐ ***Change case inputs reviews.***

- *Basic event parameter variables*. 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 probability/rate
  - Mission time
  - Calculation type
  - Process flag
- *"True" vs. 1.0.* 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.

- *Basic events with multiple uses.* 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 recovery rules (see below)

- *Recovery rules.* 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 Technical Specifications, 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 sets 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.

- Note: Keep in mind that recovery event of failed or degraded SSC may have been set to 1.0 in a previous step.

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

- 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.

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

☐ ***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 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 in this appendix, the initial model solution was ran with the non-recovery 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 “recovery 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.

Some considerations for crediting and applying recovery include the following:

☐ Refer to the handbook section in Volume 1 on modeling recovery and repair actions in event assessment for details.

☐ 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.
- 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.

☐ ***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, common-cause failure probabilities, human error probabilities, non-recovery probabilities).

Two sampling techniques are provided in SAPHIRE (Version 7) 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 handbook Section 2.2 in Volume 3 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, 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 5 and 95 percent 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 non-recovery actions added to the initial analysis cut sets, are defined in terms of probability distributions [except basic events assigned a probability of 1.0 (point value)].

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

- The SAPHIRE instructions for performing an uncertainty analysis of SPAR model parameters can be found in the SAPHIRE training manuals (Refs. 1, 2, and 3).

- 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.

☐ Refer to a future handbook section on uncertainty and sensitivity analyses for details.

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 (Ref. 14). 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:

☐ ***Every statement should have a basis.***

- 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.

☐ ***The facts.***

- Facts most important to the risk should be stated first.

- For initiating event analyses, all off-normal conditions should be stated.

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

☐ ***The 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.

☐ ***The model 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.
- Better to attach markups of effective pages from the plant SPAR model manual, such as:
  - Fault tree and event tree figures and descriptions
  - Parameter tables
  - HRA method worksheets
  - Plant diagrams (note: avoid physical layout and floor plans that may be classified as SUNSI).
- Document the revisions and dates of the SPAR model and SAPHIRE/GEM code.

☐ ***The results.***

- Summarize the results, including the results of sensitivity and uncertainty analyses.
- Attach the SAPHIRE/GEM printout, as appropriate.

☐ ***The references.*** List of reference should include the following:

- 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.

References

1. U.S. Nuclear Regulatory Commission, “Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE): Tutorial,” NUREG/CR-6952, Vo. 4, September 2008. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6952/

2. Idaho National Laboratory, “SAPHIRE Basics - An Introduction to Probabilistic Risk Assessment via the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software,” January 2005 or current revision.

3. Idaho National Laboratory, “Advanced SAPHIRE - Modeling Methods for Probabilistic Risk Assessment via the Systems Analysis Program for Hands-On Integrated Reliability Evaluations (SAPHIRE) Software,” March 2005 or current revision.

4. U.S. Nuclear Regulatory Commission, “Handbook of Parameter Estimation for Probabilistic Risk Assessment,” NUREG/CR-6823, September 2003. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6823/

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

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

7. U.S. Nuclear Regulatory Commission, “Common-Cause Failure Database and Analysis System: Event Collection, Classification, and Coding,” NUREG/CR-6268, Revision 1, Draft.

8. U.S. Nuclear Regulatory Commission, “The SPAR-H Human Reliability Analysis Method,” NUREG/CR-6883, August 2005. http://www.nrc.gov/reading-rm/doc-collections/nuregs/contract/cr6883/

9. U.S. Nuclear Regulatory Commission, “Evaluation of Human Reliability Analysis Methods Against Good Practices,” NUREG-1842, March 2006. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1842/

10. U.S. Nuclear Regulatory Commission, “Good Practices for Implementing Human Reliability Analysis,” NUREG-1792, April 2005. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1792/

11. Idaho National Laboratory, “SAPHIRE Users Group,” https://saphire.inl.gov/, June 2009, User Area Accessible to NRC-Authorized Account Holders Only.

12. U.S. Nuclear Regulatory Commission, “Technical Basis and Implementation Guide for A Technique for Human Event Analysis (ATHEANA),” NUREG-1624, Rev. 1, May 2000. http://www.nrc.gov/reading-rm/doc-collections/nuregs/pubs/

13. U.S. Nuclear Regulatory Commission, “ATHEANA User’s Guide,” NUREG-1880, June 2007. http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr1880

14. Idaho National Laboratory, “P-501 Advanced Risk Assessment Topics: Addressing Key Issues in the Development and Use of PRA for Decision Making Activities,” October 2007.

15. U.S. Nuclear Regulatory Commission, “A Review of NRC Staff Uses of Probabilistic Risk Assessment,” NUREG-1489, March 1994.

This page intentionally left blank

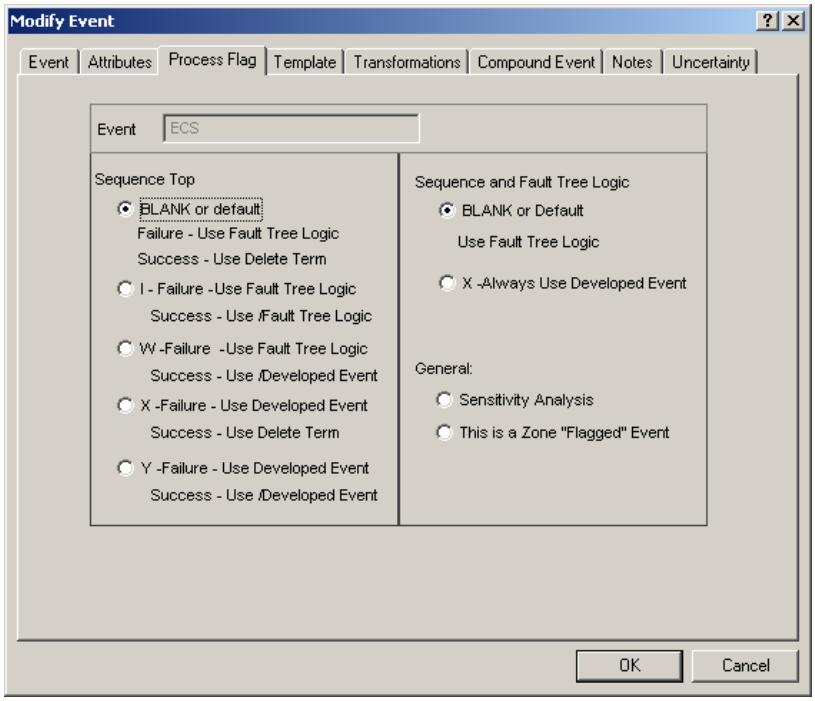
Appendix B – Quick Reference Guide: SAPHIRE Version 7

Guides

1. Process Flags

- In event trees, Process Flags are special identifiers that tell SAPHIRE Version 7 how to treat top events in various ways. For example, SAPHIRE Version 7 has one Process Flag that uses a top event as a split-fraction probability rather than as a link to its fault tree logic.

- The process flag is entered in the **Modify** → **Basic Event** option. Once in that option, highlight the basic event to be modified, click the right mouse button, select **Modify**, and then click the **Process Flag** tab.



- Both the fault tree and event tree top events show up in the list of basic events.

- The process flag field is one character long (I, W, X, or Y) and is indicated via a radio button. The process flag has different characteristics depending on the sequence branch path (recall that an up branch is success while a down branch is failure). The process flag fields are defined below.

- Any combination of top events with process flags could be used as needed. However, care should be taken since some combinations of process flags could result in questionable results.

  Example: If an event tree top event is treated as a basic event (via the **Y** process flag) but is not independent of other top events, it is possible to obtain non-conservative results due to double counting of basic events.

- The " " (space) process flag gets the most use since this is the default flag.

- The **I** flag is used when the analyst wants to see the success basic events in the cut sets. This flag is typically used for fault trees with a single basic event.

- The **Y** flag is used when the analyst only wants to use a split fraction for the top event. Note that in the next section, the “large event tree methodology,” a technique for using split-fractions for each top event in the event tree will be demonstrated.

- The **W** and **X** flags are not used that often when solving sequence cut sets.