Risk Assessment of Operational Events

Handbook

Volume 1 – Internal Events

Exposure Time Modeling – Failure Modeling
Multi-Unit Considerations – Analysis Road Map

Revision 1.01

January 2008

SDP Phase 3 ● ASP ● MD 8.3
TABLE OF CONTENTS

ACRONYMS ........................................................................................................................... v

1.0 Introduction .................................................................................................................. 1
  1.1 Objectives ................................................................................................................. 1
  1.2 Scope of the Handbook ......................................................................................... 1
  1.3 Audience for the Handbook ............................................................................... 2
  1.4 Handbook Content ............................................................................................... 2
  1.5 Companion References to the Handbook ............................................................ 3
  1.6 Future Updates to the Handbook ........................................................................ 4
  1.7 Questions, Comments, and Suggestions .............................................................. 4
  1.8 References ............................................................................................................. 5

2.0 Exposure Time Determination and Modeling ........................................................... 1
  2.1 Definitions ............................................................................................................... 1
  2.2 Exposure Time = t + Repair Time ........................................................................ 2
  2.3 Exposure Time = t/2 + Repair Time ...................................................................... 2
  2.4 Exposure Time for Component Run Failures ....................................................... 3
  2.5 Special Case for Equipment Running During a LOOP ........................................ 4
  2.6 Exposure Time for Continuous Component Operation Failures ....................... 4
  2.7 Exposure Time > One Year .................................................................................. 4
  2.8 Exposure Time for Concurrent Conditions ......................................................... 5
  2.9 Exposure Time for T/M Contribution ................................................................ 5
  2.10 References ......................................................................................................... 5

3.0 Failure Determination and Modeling ......................................................................... 1
  3.1 Types of Failure Modeling .................................................................................... 1
  3.2 Component Failure Modeling in Event Analysis ................................................. 3
  3.3 Failure Mode Definitions in SPAR Models .......................................................... 5
  3.4 Modeling Failures and Degradations in SAPHIRE/GEM ..................................... 6
  3.5 References ......................................................................................................... 10

4.0 Mission Time Modeling ............................................................................................... 1
  4.1 Mission Times in SPAR Models .......................................................................... 1
  4.2 Mission Times < 24 Hours .................................................................................... 1
  4.3 Which Mission Time to Use: SPAR or PRA ......................................................... 3
  4.4 Making Changes in SAPHIRE Version 7 .............................................................. 3
  4.5 References ......................................................................................................... 4

5.0 Test and Maintenance Outage Modeling .................................................................... 1
  5.1 Modeling T/M Events in Event Analysis .............................................................. 1
  5.2 T/M Events in SPAR Models ............................................................................... 1
  5.3 Modeling T/M in SAPHIRE/GEM (Version 7) ...................................................... 1
  5.4 Inspection of Cut Sets ......................................................................................... 3

6.0 Recovery Modeling of Failed Equipment .................................................................... 1
  6.1 Introduction .......................................................................................................... 1
  6.2 Crediting Recovery in Event Analysis .................................................................. 1
  6.3 Recoveries Modeled in SPAR Models ................................................................. 2
LIST OF TABLES

Table 2-1. Examples of exposure times for concurrent conditions. ................................................. 2-6
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ac</td>
<td>alternating current</td>
</tr>
<tr>
<td>AFW</td>
<td>auxiliary feedwater</td>
</tr>
<tr>
<td>ASP</td>
<td>accident sequence precursor</td>
</tr>
<tr>
<td>BWR</td>
<td>boiling water reactor</td>
</tr>
<tr>
<td>CCF</td>
<td>common-cause failure</td>
</tr>
<tr>
<td>CCCG</td>
<td>common cause component group</td>
</tr>
<tr>
<td>CDF</td>
<td>core damage frequency</td>
</tr>
<tr>
<td>CDP</td>
<td>core damage probability</td>
</tr>
<tr>
<td>dc</td>
<td>direct current</td>
</tr>
<tr>
<td>EDG</td>
<td>emergency diesel generator</td>
</tr>
<tr>
<td>EFW</td>
<td>emergency feedwater</td>
</tr>
<tr>
<td>EOP</td>
<td>emergency operating procedure</td>
</tr>
<tr>
<td>EPIX</td>
<td></td>
</tr>
<tr>
<td>FTR</td>
<td>failure to run</td>
</tr>
<tr>
<td>FTS</td>
<td>failure to start</td>
</tr>
<tr>
<td>GEM (code)</td>
<td>Graphical Evaluation Module (code)</td>
</tr>
<tr>
<td>HPCI</td>
<td>high-pressure core injection</td>
</tr>
<tr>
<td>HPI</td>
<td>High-pressure injection</td>
</tr>
<tr>
<td>HRA</td>
<td>human reliability analysis</td>
</tr>
<tr>
<td>HVAC</td>
<td>heating, ventilation and air conditioning</td>
</tr>
<tr>
<td>IA</td>
<td>Instrument air</td>
</tr>
<tr>
<td>LOCA</td>
<td>loss-of-coolant accident</td>
</tr>
<tr>
<td>LOIA</td>
<td>loss of instrument air</td>
</tr>
<tr>
<td>LOOP</td>
<td>loss of offsite power</td>
</tr>
<tr>
<td>LPSI</td>
<td>low-pressure safety injection</td>
</tr>
<tr>
<td>MD 8.3</td>
<td>Management Directive 8.3</td>
</tr>
<tr>
<td>MFW</td>
<td>main feedwater</td>
</tr>
<tr>
<td>NPSH</td>
<td>net positive suction head</td>
</tr>
<tr>
<td>NR</td>
<td>nonrecovery</td>
</tr>
<tr>
<td>PCS</td>
<td>power conversion system</td>
</tr>
<tr>
<td>PWR</td>
<td>pressurized water reactor</td>
</tr>
<tr>
<td>PI</td>
<td>performance indicator</td>
</tr>
<tr>
<td>RADS</td>
<td>Reliability and Availability Data System</td>
</tr>
<tr>
<td>RCIC</td>
<td>reactor core isolation cooling</td>
</tr>
</tbody>
</table>

ACRONYMS
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHR</td>
<td>residual heat removal</td>
</tr>
<tr>
<td>ROP</td>
<td>Reactor Oversight Process</td>
</tr>
<tr>
<td>SAPHIRE</td>
<td>Systems Analysis Programs for Hands-on Integrated Reliability Evaluations</td>
</tr>
<tr>
<td>SBO</td>
<td>station blackout</td>
</tr>
<tr>
<td>SDP</td>
<td>Significance Determination Process</td>
</tr>
<tr>
<td>SPAR (model)</td>
<td>Standardized Plant Analysis Risk (model)</td>
</tr>
<tr>
<td>SSC</td>
<td>structures, systems and components</td>
</tr>
<tr>
<td>SSU</td>
<td>safety systems unavailability</td>
</tr>
<tr>
<td>T</td>
<td>exposure time</td>
</tr>
<tr>
<td>T/M</td>
<td>test and maintenance</td>
</tr>
<tr>
<td>TS</td>
<td>Technical Specifications</td>
</tr>
<tr>
<td>TDAFW</td>
<td>turbine-driven auxiliary feedwater</td>
</tr>
</tbody>
</table>
1.0 Introduction

1.1 Objectives

The first objective of the Risk Assessment of Operational Events Handbook (sometimes known as “RASP Handbook” or “handbook”) was 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 was 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 in the Accident Sequence Precursor (ASP) Program (since 1969) 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 between 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 may 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 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. The analyst 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 the 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.

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
- Recovery of Failed Equipment Modeling
- Multi-Unit Considerations Modeling

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

- Roadmap - Risk Analysis of Operational Events

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. A future revision of the handbook will integrate all volumes of the handbook.

- **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,

---

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.
external fire, high winds, tornado, hurricane, and others. This volume is intended to complement Volume 1 for Internal Events.

Specifically, this volume provides the following guidance:

- Internal Flood Modeling and Risk Quantification
- Internal Fire Modeling and Risk Quantification
- Seismic Event Modeling and Seismic Risk Quantification
- Other External Events Modeling and Risk Quantification

Volumes 1 and 2 update the staff guidance that was provided for trial use in 2005 and 2006, respectively.

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 ASME PRA Standard (ASME RA-S-2005, Ref. 1-2), Regulatory Guide 1.200 (Ref. 1-3), and experiences and lessons learned from the SDP and ASP analyses.

In addition, this volume summarizes key assumptions in a SPAR model and unresolved technical issues that may produce large uncertainties in the analysis results. The importance of these assumptions or issues depends on the sequences and cut sets that were impacted by the operational event. Additionally, plant-specific assumptions and issues may play an even larger role in the analysis uncertainties.

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:

- NUREG/CR-6268, Rev. 1, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding” (Ref. 1-4)
- NUREG/CR-6850, “EPRI/NRC-RES Fire PRA Methodology for Nuclear Power Facilities, Volume 2: Detailed Methodology” (Ref. 1-5)
- NUREG/CR-6883, “SPAR-H Human Reliability Analysis Method” (Ref. 1-6)
- Basic SAPHIRE training manual (Ref. 1-8)
- Advanced SAPHIRE training manual (Ref. 1-9)
- 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 Determination and Modeling
  - SPAR-H Human Reliability Analysis Method
  - Parameter Estimation and Update Methods
  - Convolution of Failure to Run Parameters Method
  - Uncertainty Analysis Method
  - Simplified Expert Elicitation Method

  **Tutorials and examples**
  - Internal Events Modeling of Conditions and Initiating Events – Examples
  - Quick Reference Manual – SPAR Models
  - Tutorial - Common-Cause Failure Modeling
  - Tutorial - NRC's Risk Databases and Calculators

- **Future volumes.** Two additional volumes are planned in the near future:

  - Risk Analysis of Low-Power and Shutdown Events
  - Risk Analysis of Events Involving Containment-Related Events (LERF)

1.7 Questions, Comments, and Suggestions

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

**Internal NRC staff and NRC contractors:**

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

**External NRC (e.g., public, licensees):**

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


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 Graphical Evaluation Module (GEM) code calls this the “event duration” time (in hours).

- **Repair time.** Repair time is the time between discovery of the failure and when the component was placed back into service. 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.
  
  - 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 placed back into 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 mission time.

- \(\sum\text{(run times)} > \text{mission time, inception time known or NOT known}\). The exposure time starts at the time when the component no longer had the capability to operate for the mission time (usually 24 hours). This approach could be conservative if the unknown inception time of the degradation mechanism was actually after the calculated beginning of the exposure time.

For example, consider a component with a 24-hour mission time and 4 successful tests of 4 hours of run time each (for a total of 16 hours). While operating on a demand signal, the component failed to run after 12 hours of operation. The exposure time should start at the end of the first test (12 h + 4 h + 4 h + 4 h = 24 h). The calendar time between the end of the first test (e.g., clocks starts when the component was returned to service following the first test) to the time when the repaired component was placed back into service should be the exposure time. The component would have operated successfully for greater than the 24-hour mission time had the component with the degradation been demanded before the first test.
2 Exposure Time Determination and Modeling

- **\( \sum \text{(run times)} < \text{mission time}, \text{inception time known} \).** 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 component's mission time, the exposure time should start at the time of inception and end when the repaired component was placed back into service.

  Note: For the case where the inception time is NOT known, the case "\( \sum \text{(run times)} > \text{mission time and inception time known} \)" would apply.

- Repair time is included in the exposure time.

2.5 Special Case for Equipment Running During a LOOP

- In the previous section, a failure to run at any time during a 24-hour mission time was considered to be a mission failure. For most initiating events, this is consistent with the accident sequence and the generally accepted probabilistic risk assessment approach to ensure that the core is cooled for 24 hours. However, this approach can lead to overly conservative results for emergency diesel generators (EDGs) and turbine driven pumps (TDPs) in loss of offsite power (LOOP)-initiated sequences because there is a high probability of recovering from the LOOP in much less than 24 hours. The EDGs and TDPs are very important for mitigating the consequences of a LOOP event before offsite power is recovered. However, after the recovery of offsite power, the EDGs are not important. In addition, for pressurized water reactors, the turbine-driven auxiliary feedwater (AFW) pump is equally important to the redundant motor-driven AFW pumps.

  To account for the risk differences between early and late failures for EDGs and TDPs, a segmented approach can be used. This segmented approach accounts for successful run tests that occur after the inception of the degradation mechanism. The details describing the segmented approach will be provided in a future section of this handbook (Revision 2).

- For an example, refer to ASP analysis 382/03-002 from the ASP database (Ref. 2-1).

2.6 Exposure Time for Continuous Component Operation Failures

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

2.7 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 program-specific procedure.

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

  - The “\( t/2 + \text{repair time} \)" 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).

### 2.8 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).
- Table 2-1 provides examples of exposure times for concurrent conditions.

### 2.9 Exposure Time for T/M Contribution

- This category includes the addition of an exposure time segments involving a failed/degraded component and a concurrent unavailability of a component in test or maintenance (T/M) due to an unrelated cause.
- For a component in test or maintenance where there is no prior knowledge that a failed condition existed in that component and where no failure was discovered in that component during testing and maintenance, assume an exposure time segment involving the component in test or maintenance equal to the time period that the component was tagged out-of-service.
- The maintenance performed during shutdown is not included in the determination of component unavailability during power operation.
- If a scheduled T/M discovered a degraded condition, then include the T/M outage time, as well as the repair time, in the exposure time.
- Table 2-1 provides examples of exposure times for T/M contributions.

### 2.10 References

Table 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.

<table>
<thead>
<tr>
<th>Train A: failure + repair time</th>
<th>t = 0</th>
<th>Train B: T/M (unrelated cause B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exposure Time</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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):

Case B.1 - If both failures were related to the same performance deficiency, then the exposure time is the sum of the three segments. (Applies to SDP and ASP analyses)

Case B.2 - If both failures are NOT related to the same performance deficiency, then the exposure time is the sum of the three segments. (Applies to ASP analysis only)

<table>
<thead>
<tr>
<th>Train A: failure + repair time</th>
<th>t = 0</th>
<th>Train B: failure + repair time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exposure Time - Segment A</td>
<td></td>
<td>Exposure Time - Segment B</td>
</tr>
<tr>
<td>(same or different deficiencies)</td>
<td>Exposure Time - Segment C</td>
<td></td>
</tr>
<tr>
<td>(same or different deficiencies)</td>
<td>(same or different deficiencies)</td>
<td></td>
</tr>
</tbody>
</table>

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 C.1:

<table>
<thead>
<tr>
<th>Train A: failure + repair time</th>
<th>Train B: failure + repair time</th>
</tr>
</thead>
<tbody>
<tr>
<td>t=0</td>
<td></td>
</tr>
<tr>
<td>Exposure Time: Segment A</td>
<td>Exposure Time: Segment B</td>
</tr>
<tr>
<td>(same deficiency)</td>
<td>(same deficiency)</td>
</tr>
</tbody>
</table>

Case C.2:

<table>
<thead>
<tr>
<th>Exposure Time: Analysis A</th>
<th>Exposure Time: Analysis B</th>
</tr>
</thead>
<tbody>
<tr>
<td>(different deficiencies)</td>
<td>(different deficiencies)</td>
</tr>
<tr>
<td>(Not added)</td>
<td></td>
</tr>
</tbody>
</table>
### 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)

<table>
<thead>
<tr>
<th>Train A: failure + repair time</th>
<th>Train B: failure + repair time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Case D.1:</strong> Exposure Time: Segment A (same deficiency)</td>
<td>Exposure Time: Segment B (same deficiency)</td>
</tr>
<tr>
<td><strong>Case D.2:</strong> Exposure Time: Analysis A (different deficiencies)</td>
<td>Exposure Time: Analysis B (different deficiencies)</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Train A: T/M</th>
<th>Train A: failure due to T/M + repair</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>t = 0</strong> Exposure Time</td>
<td></td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Train A: T/M</th>
<th>Train A: failure (unrelated to T/M activities) + repair</th>
<th>Train A: T/M</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>t = 0</strong> Exposure Time</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Train A: failure #1 repair</th>
<th>Train A: failure #2 due to repair of previous failure + second repair</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>t = 0</strong> Exposure Time (Independent)</td>
<td></td>
</tr>
</tbody>
</table>
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.** Component malfunction events are classified into one of the following three event severity categories: catastrophic failures, degraded failures, and incipient failures (Ref. 3-1).

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

- **Degraded failures.**
  - **Degraded failures** can prevent a system or train from meeting the success criteria modeled in the PRA.
  - **Degraded failures** of structures, systems or components 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).
3 Failure Determination and Modeling

- Setting the basic event to its nonrecovery probability 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 in the ASME PRA Standard (ASME RA-Sb-2005), 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 the valve 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 structures, systems, or components that rarely fail. For a condition analysis, a structure, system or component 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 assumption 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.
3 Failure Determination and Modeling

- 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 recovery modeling of failed equipment 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 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, exponential, or catastrophic at the time of failure.

- **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\(^2\) 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. 3-5). The failure modes and component boundary definitions are also documented in Appendix A.
  - Modeling limitations that exclude failure modes can be found in the fault tree section in the plant-specific SPAR model manual (Section 4).

- **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.

---

\(^2\) Failure modes used in the SPAR models were identified in the RES system and component reliability studies. See Ref. 3-2 for details. Data used to estimate failure probabilities are primarily from EPIX failure reports. The results were estimated using the RADS calculator. Analysis methods are documented in the parameter estimation handbook NUREG/CR 6823 (Ref. 3-1).
3.2 Failure to run events in SPAR models.

- For structures, systems, and components 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 uses these same two bins. 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 structures, systems or components with two bins of failure to run modeled in SPAR models typically include:
  - Turbine-driven pumps
  - Positive-displacement pumps
  - Motor-driven pumps
  - Engine-driven pumps
  - Diesel-driven pumps
  - Motor-driven compressors
  - Heating, ventilation, and air conditioning (HVAC) fans
  - Chiller units
  - Air Handling/Heating Units
  - Gas turbine generators
  - EDGs

- Note: The binning of data may change in the future based on statistical 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 Section 2.8 of Volume 3 of the RASP Handbook for details.

- Potential for common cause. Once a component failure has been determined, then one of three determinations regarding the potential for a common-cause failure (CCF) should be made by the analyst:
  - Failure from unknown or random cause(s),
  - Independent failures, and
  - Potential common-cause failure.

In general, the common-cause probability for three cases above will follow the relationship:

\[ P(\text{CCF / common-cause failure}) > P(\text{CCF / unknown failure}) > P(\text{CCF / independent}) \]
Modeling component failure from unknown or "random" cause in SAPHIRE/GEM.

- Failures due to “random” deficiencies are the most common situation in the analyses of operational events. We know that the failed component comes from a cause included in the total failure from all causes ($A_1$), but we sometimes don’t know if it was an independent ($\alpha_1$) or potential common cause ($\alpha_2...\alpha_n$) event. The definition of an “independent” event is provided in a later section.

- If the cause of the failure cannot be determined to be independent or common-cause related (see below for guidance), then a random failure should be assumed.

- For random failures, the CCF event should be adjusted to reflect the conditional probabilities of additional failures in the common cause component group (CCCG).

The CCF event adjustment will be performed automatically in SAPHIRE Version 7 based on the following analyst’s inputs:

1. Before setting a basic event to TRUE, know where the basic event is used in the model (e.g., fault trees, recovery rules). The change may not be appropriate in all sequences.

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

   - To view where the basic event is used, from SAPHIRE Version 7: select Modify, select Basic Event, select the basic event name from the Edit Events window, and select Cross Reference.

2. Set basic event for observed failure mode (e.g., failure to start) to TRUE.

3a. If a CCCG is of size 2, set basic event representing CCF of the unobserved failure mode (e.g., failure to run) to FALSE.

3b. If CCCG is of size 3 or greater, set basic event representing CCF of the unobserved failure mode to 1.0.

Identifying an independent failure vs. random failure in event analysis. A component failure should be considered independent ONLY when the cause is well understood and there is no likelihood that the same circumstances could exist in other components in the common cause component group. Note that root cause analyses may be in error, and this possibility should be allowed for conditioning an event analysis on a presumption of zero common cause potential should be a rare occurrence.

Refer to the future handbook section on common-cause failure modeling for further discussion on the determination of independent failures.
3 Failure Determination and Modeling

- **Modeling an independent failure in SAPHIRE/GEM.**
  
  - **Important analysis note:** Modeling a failure as independent is the exception. The rule should be the "random or unknown" case. Refer to the future handbook section on common-cause failure modeling for further discussion on the determination of independent failures.
  
  - **Important SAPHIRE Version 7 note:** If the component is recoverable, the basic event should NOT be set to its nonrecovery probability. Doing so will affect the CCF calculation.

  If modeling recovery is appropriate, then add its own nonrecovery basic event to the fault tree. Refer to the handbook section on recovery modeling of failed equipment details.

  - For independent failures, the CCF event should be adjusted to effectively reduce the common cause component group size to one.

  The CCF event adjustment must be performed manually by the analyst in SAPHIRE Version 7 based on the following inputs:

  1. Before setting a basic event to TRUE, know where the basic event is used in the model (e.g., fault trees, recovery rules). The change may not be appropriate in all sequences.

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

     To view where the basic event is used, from SAPHIRE Version 7: select Modify, select Basic Event, select the basic event name from the Edit Events window, and select Cross Reference.

  2. Use nominal CCF probability for remaining components in the common cause component group. In the Graphical Evaluation Module (GEM) code, enter the baseline CCF probability calculated by SAPHIRE Version 7 before any events were set to TRUE.

     In GEM, add the basic event of interest from the Condition Assessment Events window; open the Event Probability Change window for the basic event; from the Calculation Type drop down menu, select Probability Type and enter the baseline CCF failure probability.

- **Modeling a common-cause failure in SAPHIRE/GEM.** For failure of more than one component in a common cause component group, remaining components may still fail due to either independent failures or a common-cause failure.

  Refer to the future handbook section on common-cause failure modeling for details.
Importance of process flag selection in SAPHIRE Version 7.

- **Important note:** If setting a basic event to TRUE or adjusted to a high 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 Appendix 2, Section 1, “Process Flags.”

Modeling a support system failure in SAPHIRE/GEM.

- If the support system is not included in the SPAR models, the impact of the failure on front line safety systems is addressed by setting the impacted components to TRUE.

  **Important analysis note:** The failure of the front line safety system components should be treated as independent failures so that nominal CCF probabilities are set for the unaffected components in the common cause component group.

- The modeling of a support system failure recognizes that as long as the failure remains unrecovered, all impacted structures, systems and components are unavailable; but if the support system failure is recovered, all impacted structures, systems and components may be recoverable.

- A support system failure can be modeled through multiple calculations that address the impact of failure and success of the failed support system components. Calculated core damage frequencies/probabilities for associated cut sets for each case are normalized based on the likelihood of not recovering the support system failure.

- 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 nonrecovery 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.

- **Know where the basic event is used in the SPAR model.**

  - Before setting a basic event to TRUE, know where the basic event is used in the model (e.g., fault trees, recovery rules). The change may not be appropriate in all sequences.
For example, a degraded component may not have enough capacity for one sequence (thus the reason for setting the basic event to TRUE), but may have enough capacity for success in another event tree sequence.

- To view where the basic event is used, from SAPHIRE Version 7: select Modify, select Basic Event, select the basic event name from the Edit Events window, and select Cross Reference.

- **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, such as "disallowed maintenance combinations" rule set for 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.

- **Important note:** 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 rewrite rules to produce the correct cut sets.

- **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.
  - 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.

### 3.5 References


4.0 Mission Time Modeling

4.1 Mission Times in SPAR Models

- **Typical mission times in Standardized Plant Analysis Risk (SPAR) Models.** SPAR assumes a 24-hour mission time for most structures, systems, and components. The 24-hour assumption is made for SPAR models because for many structures, systems and components, the choice is arguably conservative, yet does not contribute significantly to the top event metric. In most events, 24 hours is sufficient time to bring numerous resources to bear on core cooling. In some events, the choice is conservative and the analysis results are overestimates.

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

- **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 structures, systems, and components in a fault tree.** Mission times should be consistent with other similar structures, systems and components in a system fault tree (e.g., similar run times of motor-driven pumps).

4.2 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 revisit 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.
4 Mission Time Modeling

- **Decreasing mission time.** Mission time less than 24 hours may be appropriate for certain sequences. Mission times for individual structures, systems, or components (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 structure, system, or component may include:

- Decreasing the mission time of a structure, system, or component is more important for a structure, system, or component 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 structure, system, or component normally secured early in the sequence as the result of the use of an alternate system that is modeled as a 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.

- Emergency diesel generator (EDG) mission time based on loss of offsite power (LOOP) recovery analysis:

  - SPAR models assume a 24-hour mission time for EDGs.
  
  - *For initiating event analyses,* the EDG mission time should be the actual time that offsite power was restored to the first safety bus during the LOOP event.
  
  - *For condition analyses (where no LOOP event actually occurred),* the EDG mission time should be the mean LOOP duration time of the composite of duration-weighted average of the four individual LOOP categories (i.e., plant centered, switchyard centered, grid related, and weather related).

- **Increasing mission time.** Certain conditions involving failures, degradations, and unavailabilities may warrant increasing the mission time if already 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 (per B.5.b strategy), e.g., battery life extension.

4.3 Which Mission Time to Use: SPAR or PRA

- **Differences between the SPAR and 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 structure, system or component 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 structures, systems or components 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., structure, system, or component secured early)?
  - Does the SPAR model event tree require modification?

4.4 Making Changes in SAPHIRE Version 7

- **Important SAPHIRE Version 7 note:** Changing the mission time for a failure to run (FTR) parameter in SAPHIRE Version 7 will result in a global change throughout the model for that structure, system, or component. For template events where a generic FTR basic event is used for similar components in different systems, a change would be applied in all fault trees that use the template basic event. In most cases, the change may be applicable to one sequence or cut set. In most cases, recovery rules may be used to replace a template basic event with the mission time change.

- **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 Section 2.8 of Volume 3 of the RASP Handbook for details.

- **Making global changes in SAPHIRE Version 7.** To make a global change in the mission time of a failure to run basic 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.
• **Making specific changes using recovery rules in SAPHIRE Version 7.** Recovery rules may be developed to replace a template basic event in cut sets with a specially created basic event. 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. 4-1).

### 4.5 References

5.0 Test and Maintenance Outage Modeling

5.1 Modeling T/M Events in Event Analysis

- When modeling a component that was in test or maintenance (T/M), the desired treatment of basic events in the SPAR model is as follows:
  - No change in common-cause failure (CCF) probability of the component group of the component in T/M.
  - 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).

- Note: Treatment of a component in T/M is application specific (refer to the program-specific procedure for details).

5.2 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).

- **Sources 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.

5.3 Modeling T/M in SAPHIRE/GEM (Version 7)

- **Introduction.** SAPHIRE uses recovery rules remove cut sets to that contain combinations of equipment in test or maintenance (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.
The bottom line is that whether the T/M event is set to TRUE or 1.0, the analyst should follow up with inspection of the cut sets to see if they make sense. The numeric impacts of this issue can be significant, but are often not.

The general approach to solving this problem is to set the affected T/M event to TRUE, and to set the disallowed T/M events to FALSE so that no illogical cut sets are generated as follows:

- **View disallowed T/M combinations.** To access the disallowed T/M combinations in the SPAR model project rule file, from SAPHIRE Version 7:
  - Press the ‘Sequence’ button.
  - Select any sequence in the pop-up box.
  - Right click and select ‘Cut Sets’ in the pop-up box; select ‘Recover’ in the next pop-up box.
  - Select ‘Edit Rules’ in the next pop-up box and right click. Ensure that the radio buttons for ‘Project’ Rule Level and ‘Basic’ Rule type are selected.
  - Select ‘OK’.

- **Identify the analysis-specific disallowed T/M combinations.** You have now loaded a rules file that contains a readable computer code that eliminates disallowed T/M combinations from cut sets. The first executable computer statement generally reads “if (a long list of illogical combinations) occurs then ‘Delete Root’”. ‘Delete Root’ is simply computer command to delete the cut set containing the disallowed combinations.

This if/then statement will not work when an event is set to TRUE because the event will not appear in any cut set even though the logic propagates. Therefore, the analyst has to perform the function of the if/then statement as best shown in the following example.

For example, using the IP2 model and the T/M event (LPI-MDP-TM-21) as an example, each illogical combination involving LPI-MDP-TM-21 can be identified. By carefully examining the disallowed maintenance, we see the following:

\[
\begin{align*}
\text{LPI-MDP-TM-21} & \times \text{AFW-MDP-TM-23} + \\
\text{LPI-MDP-TM-21} & \times \text{EPS-DGN-TM-23} + \\
\text{LPI-MDP-TM-21} & \times \text{HPI-MDP-TM-23} + \\
\text{LPI-MDP-TM-21} & \times \text{LPI-MDP-TM-22} + \\
\text{LPI-MDP-TM-21} & \times \text{CCW-MDP-TM-MDP23} +
\end{align*}
\]

Thus, the events to the right of the ‘*’ cannot be at the same time in maintenance with the T/M event of interest (LPI-MDP-TM-21 in the example).

- **Note the disallowed T/M combinations.** Write down, copy, or print the basic event names from the desired disallowed T/M combination. Close all of the windows until you are back to the main SAPHIRE menu.

- **Return to the event or condition analysis.** Now proceed with the SAPHIRE or GEM analysis in a normal manner. Set the affected T/M event to TRUE, and to set the disallowed T/M events to FALSE.

In the above example, LPI-MDP-TM-21 would be set to TRUE and the illogical T/M events (AFW-MDP-TM-23, EPS-DGN-TM-23, HPI-MDP-TM-23, LPI-MDP-TM-22, and CCW-MDP-TM-MDP23) should now be set to FALSE in a SAPHIRE change set or a GEM analysis.
5.4 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.
  
  - Review each cut set.

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

  - **Disallow ed 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 emergency diesel generator (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.
6.0 Recovery Modeling of Failed Equipment

6.1 Introduction

Recovery analysis addresses the potential recovery of failed structures, systems and components and human errors prior to core damage or containment release. A complete recovery analysis is labor intensive and is only recommended for events that are of high risk significance or are controversial. For other events, a limited recovery analysis should be performed that addresses the potential recovery of equipment failure or unavailability subject to analysis as well as recovery actions already addressed in the probabilistic risk assessment (PRA) (i.e., existing recovery rules, recovery basic events or an existing recovery analysis that can be easily modified to reflect the dominant cut sets associated with the event).

6.2 Crediting Recovery in Event Analysis

- **Is recovery creditable for a condition actually observed?** Questions to consider for crediting recovery of an actual failure for the postulated sequence of interest:
  - How long did the recovery actually take? Was there any time pressure for the recover?
  - Can the crew diagnose the need for recovery for the various postulated core damage sequences? Refer to each of the performance shaping factors of the SPAR-H Method.
  - Is there enough time to recover the failed component, start the system, and recover core cooling for postulated sequences? Considerations include:
    - Time to core uncovering
    - Time to recover vessel water level before pressure exceeds injection limits (low pressure - pump runout; high pressure - pump shutoff head)
    - Time to suppression pool overpressure failure
    - Time to suppression pool temperature exceeding net positive suction head (NPSH) limits
  - Can the component be recovered within the component mission time modeled in the PRA? If not, then recovery should not be credited.
  - Would the crew know how much time is available before core uncovering or other time sensitive consideration?
6 Recovery Modeling of Failed Equipment

- Can the component be recovered given postulated extreme environmental conditions? Considerations include:
  - Steam leak/rupture
  - Flooding from line breaks (floor drains overfill, overflow down stairways)
  - High radiation levels from sump recirculation
  - Component inside containment
  - Availability of lighting during loss of offsite power scenarios

- Can the component be recovered within the needed time frame? Considerations include:
  - Tools readily available
  - Spare parts readily available
  - Plant staffing level with the right skills

Note: Full plant staffing available only 25% of the year; however, emergency response organization activated within 1 to 1.5 hours.

- Will the recovery be performed within the mean-time-to-failure duration consistent to the nominal hardware failure probability? If not, then what is the failure probability? Engineering judgment or expert elicitation may be needed to address this question.

- Are the support systems available in sequences in which recovery is credited?

- **Is recovery creditable for the accident sequences in general?** Often a condition assessment will change (or elevate) the risk importance of certain sequences from negligible to dominant. Since these sequences were negligible in the baseline risk profile from quantifying the SPAR model, recovery was not considered. In an analysis of a high-risk condition, recovery analysis is warranted when the SPAR model lacked recovery modeling.

  For example, the ASP analysis of the Point Beach condition of the common mode failure of auxiliary feedwater (AFW) pumps (Ref. 6-4) included the recovery analysis of the instrument air (IA) system, which was not directly involved in the condition involving the AFW pump trains. Recovery of IA was determined to be important in dominating sequences and the operating experience data supported crediting recovery of IA. The loss of IA event tree was modified to include recovery of IA. See the summary of this condition at the end of this section.

6.3 Recoveries Modeled in SPAR Models

- **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.

- **Basic event notation in SPAR models.** Recovery from equipment failures are modeled as human error (basic) events noted by “XHE-XL” in the basic event name.

- **Where to find recovery actions in SPAR models.** Refer to the table that summarizes human actions in the plant-specific SPAR model manual (Section 8 for boiling water
Recovery of failed equipment, Section 9 for pressurized water reactor (PWR) models) for a complete listing of recovery actions credited in the SPAR models. Recovery from equipment failures are modeled as human error (basic) events noted by “XHE-XL” in the basic event name.

- **Recovery of ac power in SPAR models.** The loss of offsite power (LOOP) and station blackout (SBO) models credit recovery of ac power (e.g., offsite power source, alternate power source, emergency diesel generator (EDG)). Offsite power nonrecovery basic events are modeled by a simple one or two basic event fault tree used as top events in the LOOP/SBO event trees. Such nonrecovery events are dependent on time and type of LOOP initiating event (i.e., plant centered, switchyard centered, grid related, weather related).

- **Nominal recovery of an EDG in SPAR models.**
  - Nominal EDG recovery during SBO. The SBO model credits recovery of an EDG. The EDG recovery event in the SPAR SBO event tree models recovery of one of two (or more) failed EDGs, with the plant personnel recovering the EDG that required the least time to recover.

    This was modeled by simulation of the failure of two EDGs (each with its own recovery time), choosing the shortest recovery time of the two for each sample. These results were then fit to a Weibull distribution with $\alpha = 0.745$ and $\beta = 6.14$ hours. The mean of this distribution is 7.4 hours and the median is 3.8 hours based on information from NUREG/CR-6890, “Reevaluation of Station Blackout Risk at Nuclear Power Plants - Analysis of Loss of Station Blackout Risk.” (Ref. 6-2)

  - Nominal EDG recovery during LOOP. EDG recovery is not credited in the LOOP model when one or more EDGs function (only credited in SBO scenarios). However, NUREG/CR-6890 (Ref. 6-2) does provide information on EDG recovery. It uses information from the Reactor Oversight Process (ROP) Safety Systems Unavailability (SSU) Performance Indicator (PI) Program for EDGs from 1998-2002 to determine a recovery time curve for an EDG. The unplanned demand data were best fit with a Weibull distribution with $\alpha = 0.739$ and $\beta = 15.50$ hours. The mean of this data distribution is 18.7 hours and the median is 9.4 hours.

- **Recovery of main feedwater in PWR SPAR models.**
  - Most PWR SPAR models credit the recovery of main feedwater (MFW) for two nominal conditions: reactor trip with safety injection (MFW-XHE-XL-ISTRIP) and without safety injection (MFW-XHE-XL-TRIP). Each nonrecovery probability was estimated using the SPAR-H Method based on generic assumptions of performance shaping factors at their nominal values.

  - For an initiating event analysis involving an actual failure of the MFW system, the SPAR-H Method should be used to estimate nonrecovery probability based on actual conditions observed during the event.
Note: Recovery of a motor-driven main feedwater pump is less complex than a turbine-driven pump. Also, some plants have a startup feedwater pump.

- **Recovery of PCS in the long term in BWR SPAR models.** Most BWR SPAR models credit the recovery of power conversion system (PCS) for various initiators. The recovery probability values used are estimates based on generic data and should be reevaluated if the recovery of PCS becomes important.

- **Recovery of RCIC and HPCI in BWR SPAR models.**
  - BWR SPAR models credit the recovery of reactor core isolation cooling (RCIC) and high-pressure coolant injection (HPCI) systems for various failure modes. The recovery probability values for these events are based on the NRC system reliability studies (Ref. 6-1).
  - The HPCI and RCIC nonrecovery events are summarized in the table listing human actions in the plant-specific SPAR model manual (Section 8).
  - Dependency between the HPCI and RCIC system recovery events in SPAR models:
    - The RCIC recovery failures are assumed to occur first and therefore, considered to be independent.
    - The HPCI recovery events are considered to be dependent on the RCIC events in the combinations shown in the table of dependent human actions in the plant-specific SPAR model manual (Section 8).
    - Dependency between recovery events other than those in the HPCI/RCIC systems is considered negligible, as is dependency between recovery events and operator actions to align and control systems.

- **Recovery of AFW in PWR SPAR models.**
  - PWR SPAR models credit the recovery of AFW system for various failure modes. The values for these events are based on the NRC system reliability studies. (Ref. 6-1) The AFW recovery events are summarized in the table listing human actions in the plant-specific SPAR model manual (Section 9).
  - Dependency among the hardware recovery events was taken into account. It was assumed that the recovery events were completely dependent upon one another and only one hardware recovery could be performed per cut set. Therefore, multiple AFW hardware recovery events were pruned down to contain only one per cut set. The rules for performing this pruning operation are listed in the SPAR model manuals.

- **Recovery from support system initiators.** Recovery from losses of various support systems (e.g., instrument air, service water, component cooling water) is typically credited in SPAR model event trees.
The support system nonrecovery events are summarized in the table listing human actions in the plant-specific SPAR model manual (Section 8 for BWR models, Section 9 for PWR models).

The nonrecovery probability values used are generic estimates and should be reevaluated if the recovery of the system becomes important.

6.4 Recovery Modeling Considerations

- **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 Section 2.8 of Volume 3 of the RASP Handbook for details.

- **Find recoverable cut sets in SAPHIRE/GEM.** Some sequences may be suppressed due to the inclusion of multiple actions. Setting all recovery actions to a failure probability of 1.0 and re-quantifying will identify important sequences that contain one or more operator actions. This approach will enable the review of these recovered sequences to ensure that the treatment of recovery actions is appropriate.

- **Consider support system availability.** Ensure that support systems are available in the sequences in which recovery is credited.

- **Review recovery rules in SAPHIRE Version 7.**
  - 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 event being analyzed and modify as necessary.
  - Recovery rules may be applied to a particular fault tree, all fault trees, a particular event tree sequence, or all event tree sequences.
  - Access the recovery rules and review the logic to ensure the rules are appropriate. To view the rules: in SAPHIRE Version 7,
    - Select Sequence
    - Select and right click any sequence from the Sequence window
    - Select Cut Sets, Recover, and Edit Rules from the menus
    - Select the Project button from the Edit Recovery Rules window

- **Review nonrecovery basic events.**
  - Nonrecovery basic events included in the fault trees that appear in the cut sets should be reviewed to confirm that the nominally assigned probabilities are appropriate, considering the cut set structure.
  - Cut sets should be reviewed for multiple recovery actions as discussed in the "Multiple Recovery Actions" subsection.
6 Recovery Modeling of Failed Equipment

- If more than one nonrecovery event exists within a cut set, set only one to its nominal probability unless a review of the cut set indicates that adequate time permits the recovery of more than one failed structure, system, or component.

- **Use of HRA vs. operating experience data.**
  - Human reliability analysis (HRA) is best used to model recovery of an actual failure, where the failure mechanism is known and recovery is feasible. The preferred method for HRA is the SPAR-H Method. Plant-specific data and plant-specific considerations should be applied in the SPAR-H Method to estimate recovery from a particular failure or failure mode observed in the event in question.
  - The use of generic, industry-wide operating experience data is best suited for estimating a nominal nonrecovery probability of a postulated failed structure, system, or component or a nonrecovery of postulated initiating event (e.g., recovery from the loss of instrument air).

- **Nominal nonrecovery probability based on operating experience data.** Nominal nonrecovery probabilities are usually based on generic, industry-wide operating experience failure data. Each failure is reviewed for potential recovery and a failure probability is estimated based on the ratio of number of potential non-recoveries to total number of failures. Some considerations:
  - Refer to the NRC system reliability studies for nonrecovery probabilities that were generated for select failure modes in various systems. A potential recovery was credited in these studies when the recovery can be performed from the control room. These studies can be found on the NRC Reactor Operational Experience Results and Databases web site (Ref. 6-1). Examples include restart of a turbine-driven pump following overspeed trip and closing an EDG output breaker following a spurious trip (open). An engineering evaluation should confirm that restarts could have worked (with nominal failure probabilities) for the event being analyzed.
  - Understand how potential recoveries were classified. Creditable recovery actions listed above should be used to consider whether to include the nonrecovery probability in the analysis.
  - Use of system-specific data is preferred over pooling data across system boundaries. In some cases, pooling of data is acceptable given strong evidence that component's maintenance, operation, and performance conditions are similar. Refer to the NRC component performance studies (Ref. 6-1) for comparison of similar components.
  - A Jefferys Noninformative Prior in a Bayes Update Distribution should NOT be used to estimate a nominal nonrecovery probability of a failure mode based on no observed or potential recoveries in the operating experience. If potential recoveries were not observed in the operating experience, then the nominal nonrecovery should not be modeled (or it should be assumed to be 1.0). Assuming that potential recovery is possible without evidence to support the assumption may be a non-realistic assumption.
Review multiple recovery actions. Considerations for crediting and modeling multiple recovery actions include the following:

- Recovery should be limited to one component in the 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.

- Recovering two independent failures in two systems may be a burden on plant staff, except when ample time exists to recover two failures or the recovery of one of two failures is a simple reset action (control room or local).
  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. Quick recoveries involving trip resets from the control room may allow operators to diagnose and recover another system failure.

- Check for more than one hardware recovery in a cut set to determine whether such credit is reasonable.

- Look for multiple human actions in cut sets for reasonable combinations. The focus of the review should be the following:
  - Credit of recovery actions. See the above subsection “Is recovery creditable?”
  - Dependency among all human actions in the cut set.

Recovery from failure to run (FTR). 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 extends the time before core uncovery, and this allows for more recovery 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 from an FTR event:

- Alternate mitigating strategies. FTR is most likely due to a catastrophic failure, so recovery of the failed component during the accident sequence may not be possible. However, recovery of the accident sequence with the use of an alternate mitigating strategy maybe possible within the extended time frame.

- Increase in the “time available” for diagnosis and operator actions in HRA. Extended time may increase the “time available” performance shaping factor category level in the human reliability analysis of routine operator actions in some sequences.
  For example, failure of all AFW at 3 hours after reactor trip would increase the available time to initiate feed and bleed actions.
6 Recovery Modeling of Failed Equipment

- **Thermal-hydraulic bases 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/uncouvery times) used in event trees are usually based on the assumption that failure to start (FTS) and FTR events occur at \( t = 0 \). The success criteria used in event tree and fault tree models are based on sequence timings that are estimated from thermal-hydraulic analyses.

- **Reduced mission time.** A recovery from FTR will reduce the mission time that the component/system has to run, after recovery, to complete its 24-hour mission.

- **Adding a nonrecovery event in SAPHIRE Version 7.**
  - **Update the base case.** When adding a nonrecovery event to a fault tree using SAPHIRE Version 7, make sure that the base case model is updated, as well as the current case model. Otherwise, a negative importance may be calculated in some sequences due to a lower core damage probability (CDP) or core damage frequency (CDF) of the base case SPAR model.
  - **Use the correct fault tree logic.** Verify that the correct logic is used to model the recovery in the fault tree.
    - Nonrecovery event (e.g., NR-FTS) is “ANDed” with the failure mode event (e.g., FTS).
      
      For example: \((NR-FTS * FTS)\).
    - Nonrecovery of a new failure mode (e.g., NR-FTObreaker) is ANDed with the new failure mode (e.g., NR-FTObreaker); however, the new failure mode is ORed with existing failure modes (e.g., FTS)
      
      For example: \([\left(\left\{\left\{\text{NR-FTS} * \text{FTS}\right\}\right\} + \left\{\text{NR-FTObreaker} * \text{FTObreaker}\right\}\right]\). In this example, ensure that the “old” failure mode does not contain failure events relating to the new failure mode.
  - **Include nominal failures with the recovery.** When modeling the recovery of an actual failure, include nominal probability of hardware failures, as well as the nonrecovery probability. Components can FTS and FTR after they are recovered and restarted. This is important for failure modes with high failure probabilities. Since the component event is set to TRUE, a subtree is needed to model the recovery and operation of the component throughout its new mission time.
  - **Process Flag.** When modifying a fault tree that results in a high failure probability (e.g., 0.1 to 1.0) in an event tree top event, 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 the SAPHIRE Version 7 Training Manual (Ref. 6-3).
- **Dependencies and impossible combinations.** Look for dependencies and impossible combinations in cut sets with multiple human error events, especially when two human error events involve recovery actions. The SPAR-H Human Reliability Analysis Method provides guidance for the evaluation of dependencies of creditable multiple recovery human error events in a cut set (Ref. 6-4).

- **Recovery modeled in other PRAs.** If the PRA model includes a recovery analysis, review its nonrecovery events and their development for applicability to the event analysis. Update relevant dominant cut sets associated with the event.

- **Recover, re-sort, and examine cut sets.**
  - Include operator recovery actions that can restore the functions, systems, or components on an as-needed basis to provide a more realistic evaluation. Consider recovery of significant sequences. (ASME PRA Standard defines significant as 95% of the baseline risk profile.)
  - Re-sort cut sets as necessary to identify those that rank in the upper 95th percentile. The relative significance of cut sets will be reduced when relevant recovery credit is applied to the specific cut sets.
  - Examine a sample of non-dominant (bottom) cut sets, to make sure that they are really non-dominant (i.e., it's possible, by applying an inappropriate recovery event, to push a dominant cut set below the lower 5th percentile).

### 6.5 Examples

- **Recovery from LOIA using data.** An initiating event involving the loss of instrument air (LOIA) initiator is modeled in an event tree in some SPAR models, but the recovery is not modeled. In the ASP analysis of the Point Beach common-mode failure the AFW system (266/01-005), the industry-wide operating experience was reviewed for recovery of actual LOIA events.

  The operating experience showed that instrument air losses are recovered within a short time following reactor trips (within 4 to 30 minutes). A review of the data revealed that instrument air failures are detected prior to reactor trip and easily restored shortly thereafter (the reactor is usually manually tripped due to the gradual closing of the MFW regulating valves).

  The LOIA event tree was modified to include recovery of instrument air pressure in the short term (i.e., before the AFW pumps fail, in the mid-term (i.e., in time for the operators to initiate feed and bleed cooling before core damage would occur) and in the long term (i.e., in time for the operators to initiate secondary cooling using the MFW system).

  From the industry-wide data, "conditional" nonrecovery probabilities were calculated for various times following the LOIA. Conditional probabilities were used to model recovery possibilities at the various time period (i.e., short term, medium term, and long term) so that the product of the nonrecovery probabilities in a cut set does not exceed the failure probability to recover instrument air for the longest term sequence.

  Details how the data was reviewed and nonrecovery probabilities were estimated calculated for this condition is provided the ASP analysis 266/01-005 from the ASP database (Ref. 6-5).

- **Recovery from locked closed AFW valve using the SPAR-H Method.** The turbine-driven emergency feedwater (EFW) pump discharge manual-operated valve was locked in the closed position during a surveillance test. The human error probability for recovering the turbine-driven EFW pump train for SBO and non-SBO sequences was estimated using the SPAR-H Method.
The basis for crediting recovery is as follows. In an event requiring the turbine-driven EFW pump, the operators would know that a problem exists with the pump because there would be no EFW flow to the steam generators. Examining the local turbine-driven EFW pump flow and discharge pressure indications would indicate that the problem is not with the pump itself. This would prompt them to look at the downstream piping. Downstream of the pump flow indication the recirculation line branches off before a check valve and the manual isolation valve in question (XVG-1036). To open the valve, the operators must first unlock the valve handle.

Details on how the SPAR-H Method was used to estimate the nonrecovery probability for this condition is provided the ASP analysis 395/00-006 from the ASP database (Ref. 6-5).

6.6 References


6-5. 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)
7.0 Multi-Unit Considerations Modeling

7.1 Analysis Rules

- **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.

7.2 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

7.3 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.

- **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:
  
  o Consider the need to adjust the initiator frequency based on operating experience to reflect impact on two or more units.
  
  o 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).
  
  o Consider the need to modify value assignments of performing shaping factors per SPAR-H Human Reliability Analysis Method (Ref. 7-1).

7.4 **Examples**

The following ASP analysis can be viewed from the ASP database (Ref. 7-2).

• 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.

7.5 **Other Suggested Readings**


7.6 **References**


Appendix 1 – Roadmap: Risk Analysis of Operational Events

Contents

Acronyms

1.0 Introduction
1.1 Overview
   • Process overview
   • Analysis overview
1.2 Overview of this Roadmap
   • Iterative nature of analyses
2.0 Risk Analysis of an Operational Event

Step

① Understanding the Event
   • General Documentation Considerations
   • Generic Event Information Considerations
     - Information common to all analyses
     - Information applicable to initiating event analysis
     - Information applicable to condition analysis
   • Event-Specific Information Considerations
     - Modeling Considerations - External Events (Volume 2)
② Comparison of the Event and As-Built, As-Operated Plant with the SPAR Model
③ Model Elaboration to Reflect Additional Event-Related Detail
   • Check the SPAR model assumptions
   • Event tree modification
   • Fault tree modification
   • Initiating event frequency parameter update
   • Basic event parameter update - independent failure probability
   • Basic event parameter update - common-cause failure probability
   • Basic event parameter update - human error probability
   • Solving revised model
   • Saving the revised model
④ Model Modification to Reflect the Event
   • Initiating event probability
   • Initiating event nonrecovery probabilities
   • Components determined to be failed
   • Components determined to be degraded
   • Components that were successful
   • Potential common-cause failure
   • Human error probabilities (HEP)
   • Test and Maintenance Contribution
   • Exposure time (condition duration)
Appendix 1 Road Map: Risk Analysis of Operational Events

5 Estimation of Event Significance (Initial Model Solution)
- Nonrecovery event
- Truncation value
- Condition analysis
- Overlapping conditions
- Initiating event with an observed failure

6 Review of Initial Analysis Results
- Analysis inputs
- Know where the basic event is used in the SPAR model
- Condition exposure time input
- Cut set reviews
- Multiple operator actions
- Importance measures review
- Another check

7 Recovery Analysis

8 Review of Final Analysis Results
- Inputs and assumptions
- As-built, as-operated plant
- Model modifications
- Sequences and cut sets
- Inputs, assumptions, and results

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

10 Analysis Documentation

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

The following roadmap 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 roadmap, “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.

1.1 Overview

Process overview. The overall event analysis process involves the modification of a SPAR model to reflect attributes of an operational incident, solution of the modified model to estimate the risk significance of the incident 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 analysis 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.

**Analysis overview.** 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 operational experience. 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.¹

The risk model, modified to reflect observed failures and other off-normal situations, is solved to estimate, for an initiating event, the probability of proceeding to core damage given the observed failures (conditional core damage probability).

For a degraded condition, risk significance is estimated based on the increase in core damage probability over the duration that the condition existed (conditional core damage probability - nominal core damage probability, or importance). 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.

Event analyses are performed on the failures and off-normal situations observed during the initiating event or degraded condition. All other components in the risk model that were not impacted or challenged by the operational event are modeled with nominal failure probabilities.

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).

### 1.2 Overview of this Roadmap

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

---

¹ 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.
Sections 2 through 7 in this handbook provides 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 roadmap 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 previous 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
2. Risk Analysis of an Operational Event

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 tasks throughout the analysis.

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 pieces of information should refer to a traceable reference, whether an inspection report, drawing, system description, procedure, or a discussion with NRC or plant staff member.

Generic Event Information Considerations

For all but the simplest situations the description should include a time line that details the sequence of events. Some considerations include the following:

Information common to all analyses.

- 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 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).

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
Appendix 1  Road Map: Risk Analysis of Operational Events

- 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 the 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, ergonomics issues, observed poor work processes)

Information applicable to condition analysis.

- Relevant maintenance and testing history associated with the failed or degraded structure, system or component
- Overlapping unavailability of other another component, if appropriate for the analysis application (refer to the program-specific procedure). Licensee event reports (LERs) issued at least one year before the first condition should be reviewed for other unavailabilities.

Event-Specific Information Considerations

Information useful for the analysis of external events is provided in Volume 2 of the RASP handbook. Refer to the handbook sections on modeling considerations for the following operational events:

- **Modeling Considerations - External Events (Volume 2).**
  - 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 Comparison of the Event and As-Built, As-Operated Plant with the SPAR Model

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:

- The SPAR model should be the most up-to-date model revision.
- Review model documentation to develop an understanding of the assumptions and details associated with the sequences and fault trees related to the event.
- Identify pending changes scheduled for incorporation in the model and the expected date of the next revision. Identify any changes that could impact the analysis of the event and which therefore should be incorporated as a part of the analysis.
- If available, review one-time modeling changes made in previous SDP and precursor analyses for applicability to the event.
- Confirm that 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.
- Confirm that observed or potential component/system interactions are addressed in model.
- Confirm that observed plant operating status, including support system status, can be addressed in the model.
- Confirm that the model can be configured to represent the plant status at the time of the event. If not, confirm that the modeled system configuration will not significantly impact the results of the analysis.
- For events that could only occur at low power, confirm that system success criteria are reasonable.
- Confirm that potential common-cause failures associated with impacted components are included in model.
- Confirm relevant operator actions are addressed in model.
- Confirm that mission times for important components are appropriate. Mission times should be specified based on the structure of the sequence and are typically 24 hours unless component recovery or sequence recovery through the use of an alternate system is modeled as a part of the sequence. See the handbook section on mission time modeling for further guidance.
- Important and creditable alternative mitigating strategies have been considered. Refer to Section 2.1 of Vol. 3 of the RASP handbook for criteria for crediting a new strategy.
- Refer to Section 2.1 of Vol. 3 of the RASP handbook for additional considerations for checking whether the SPAR model reflects the as-built, as-operated plant for the important sequences that are impacted by the operational event under consideration.
Step 3 Model Elaboration to Reflect Additional Event-Related Detail

Based on the information developed in the previous step, revise the base case model as necessary to reflect the risk-related features of the event. Some considerations are as follows:

- **Check the SPAR model assumptions.** Review the SPAR model assumptions (e.g., event tree, fault tree, parameter basis) in the 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 detail that may be added to the original SPAR model include:
    - Additional top events that represent initiator recovery.
    - Changes to an event tree linking rule\(^2\) that replaces 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 initiator or transfer tree.
  - Modifications to the SPAR model should be performed or reviewed by the SPAR model developer.
  - The SAPHIRE code instructions for creating and modifying event trees in the SPAR model can be found in the SAPHIRE Version 7 Training Manuals (Ref. 4).
  - 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 fault trees to incorporate additional details not included in the original model. This is typically in the form of a basic event added to a fault tree or a different fault tree linked to an event tree top event.

Some considerations for fault tree modifications include the following:

- Examples of additional detail that may be added to the original SPAR model include:
  - Actual failed or degraded component (focus of the analysis).
  - Mitigative features present in the design.

---

\(^2\) 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.
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.

- The SAPHIRE instructions for creating and modifying fault trees in the SPAR model can be found in the SAPHIRE Version 7 Training Manuals (Ref. 4).

- 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 original 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 revised base case model. Modifications to a parameter value that reflect the impact of the operational event will be performed on the SPAR model current case in the next task.

Some considerations for parameter modifications include the following:

- The reasons to change or create a new a base case parameter 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 parameter by carefully screening the operational experience database for relevant events, 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),

    - A parameter definition was revised to reflect a modification to the SPAR model, and
Appendix 1 Road Map: Risk Analysis of Operational Events

- The 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 truly 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 revised base case model.)

- Modifications to the SPAR model parameters should be performed or reviewed by analysts specializing in the data collection and parameter estimation.

- Initiating event frequencies used in SPAR models are based on the analysis methods and results\(^3\) 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).

- The SAPHIRE instructions for creating and modifying basic event parameters in the SPAR model can be found in the SAPHIRE Version 7 Training Manuals (Ref. 4).

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

Basic event parameter update - independent failure probability.

This activity involves the update, modification, or creation of a basic event parameter to incorporate additional details not included in the original base case model. A modification typically includes the update of the number of failures (numerator) and the update of the associated number of demands spanning the period of failures (denominator).

The new or modified parameter should reflect the nominal failure probability in the revised base case model. Modifications to a parameter value that reflect the impact of the operational event will be performed on the SPAR model current case in the next task.

Some considerations for parameter modifications include the following:

- The reasons to change or create a new a base case parameter 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.

\(^3\) Data used to estimate initiator frequencies are primarily from Licensee Event Reports (LER) 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. 6).
- Update a parameter with plant-specific operational experience, because the plant-specific operational experience justifies a higher or lower failure probability.

- Modify a parameter by carefully screening the operational experience database for relevant events, because
  
  - A unique plant-specific design feature makes the use of the generic industry average failure probability questionable (e.g., may not represent the as-built, as-operated plant) and
  - A parameter definition 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 data collection and parameter estimation.

• Failure probabilities used in SPAR models are based on the analysis methods and results\(^4\) 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).

• The SAPHIRE instructions for creating and modifying basic event parameters in the SPAR model can be found in the SAPHIRE Version 7 Training Manuals (Ref. 4).

• 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 original base case SPAR model. The new or modified parameter should reflect the nominal failure probability in the revised base case model. Modifications to a parameter value that reflect the impact of the operational event will be performed on the SPAR model current case in the next task.

Some considerations for parameter modifications include the following:

• The reasons to change or create a new a base case parameter may include:
  
  - Create a new CCF parameter that represents the failed/degraded component and similar components in the common cause component group. (Note: a nominal failure probability will be estimated and assigned for the revised base case model.)
  - Create a new CCF 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.

\(^4\) 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 (Ref. 6).
- 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.

- Modify a parameter by carefully screening the operational experience database for relevant events, 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) and
  
  - A parameter definition 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 data collection and parameter estimation.

- The Alpha Factor Method was used to estimate probabilities for all CCF events in the SPAR model. Common-cause failure probabilities used in SPAR models are based "CCF Parameter Estimations, 2003 Update" report (Ref. 7). The data collection and analysis methods are based on NUREG/CR-6268, “Common-Cause Failure Database and Analysis System: Event Collection, Classification, and Coding." (Ref. 2)

- When applying a CCF parameter to a fault tree model, the CCF event should closely match the CCF parameter's system and component boundary. System and component descriptions, boundaries, and failure modes are described in Ref. 7.

- It is up to the analyst to decide the level of pooling that is appropriate in the intended use. If data exist at the system/component level most appropriate to the intended use, and are not sparse, it is recommended to use the more specific data. Otherwise, it is recommended to use the industry level pooled component data. If no pooled components are listed that are similar to the intended use, the use of the No Data (Prior Only) Pooled Distribution may be appropriate.

- Section 2 of Ref. 7 labeled No Data (Prior Only) shows the prior used in the CCF database. 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.

---

5 Equipment failures that contribute to CCF events are identified during searches of Licensee Event Reports (LER), Nuclear Plant Reliability Data System (NPRDS) failure reports, and Equipment Performance and Information Exchange (EPIX) failure reports. The results were estimated using the CCF database calculator.

6 Alpha factors are provided for many components in Ref. 7. Data for most components are pooled at the component level, e.g., motor-driven pumps, manual-operated values; however, data for some components are pooled at the system level. Pooling of data into component types simplifies the SPAR model maintenance and reduces variance in the alpha factor estimates.
The SAPHIRE instructions for creating and modifying basic event parameters in the SPAR model can be found in the SAPHIRE Version 7 Training Manuals (Ref. 4).

A checklist for aiding in the review of 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 original base case SPAR model. The new or modified parameter should reflect the nominal failure probability in the revised base case model. Modifications to a parameter value that reflect the impact of the operational event will be performed on the SPAR model current case in the next task.

Some considerations for parameter modifications include the following:

- The reasons to change or create a new a base case parameter may include:
  - Create a new HEP parameter that represents
    - Nonrecovery (diagnosis and action) of the failed/degraded component or system,
    - Failed operator action (diagnosis and/or action) that was observed during the operational event,
    - Deficiency in an operating procedure, or
    - Operator action 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 error probabilities used in SPAR models are generally generic across plant designs [e.g., pressurized water reactor (PWR), boiling water reactor (BWR)]. Some exceptions account for differences in timing of a particular sequence (time to uncover the core) where the PSF for “time available” may vary for an HEP parameter. The human reliability analysis worksheet for each HEP parameter is documented in Appendix E of the plant SPAR model manual. The human reliability analysis method used to estimate HEPs in SPAR models is based on NUREG/CR-6883, “The SPAR-H Human Reliability Analysis Method” (Ref. 3).

- The SAPHIRE instructions for creating and modifying basic event parameters in the SPAR model can be found in the SAPHIRE Version 7 Training Manuals (Ref. 4).

- 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 revised model.** This activity involves the solution of the modifications to the base case SPAR model. The model solution also includes a comparison review of solution results with the original base case model by the analyst. The review should confirm expected changes in results, as well as to identify abnormalities. In addition, the review should ensure that the revised base case model reflects the documentation of changes produced in previous activities and tasks.

Some considerations for solving the revised SPAR model include the following:
- Solve the revised model using the same truncation probability as the original model.
- Compare the revised model sequence cut sets with those from the original model to confirm model revisions.
- For condition analyses, update the base model to include the new basic events and logic.

**Caution** - When updating base case model, ensure that any change sets are not saved.

☐ **Saving the revised model.** Save the revised model using a unique file name that associates the model with the event under analysis.

**Step 6 Model Modification to Reflect the Event**

In this step, model modification refers to changes in basic event probabilities that are necessary to reflect the failures, unavailabilities and other undesirable occurrences observed during an event. Modeling of logic changes necessary to reflect the event are addressed in the previous step. The main objectives of this analysis step are: define the event and modify the SPAR model to reflect the event.

Identify the event:

- **Initiating event analysis.** The actual time and cause of the event initiator are used in modeling the severity of the event. The likelihood of an event initiator should not be modified or adjusted to 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.

- **Condition analysis.** The actual time of discovery and cause of the component unavailability is used in modeling the condition. The likelihood of a modified discovery time or cause resulting in a more severe outcome or worst case should not be assumed 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.

Modify the model to reflect the event as follows:
Know where the basic event is used in the SPAR model. Check that a proposed change in a basic event parameter (e.g., failure probability, mission time, calculation type, process flag) does not adversely impact the use of the same basic event used elsewhere in the SPAR model. The change may not be appropriate in all sequences.

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

Refer to Section 2.8 of Volume 3 of the RASP Handbook for details.

Initiating event probability. The frequency of initiating events included in the PRA model need to be specified as probabilities for both degraded condition and initiating event analyses.

- 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 \((\lambda \times \text{exposure time}) < 0.1\). 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.

Initiating event nonrecovery probabilities. This activity involves the treatment of recovery from an initiator that resulted in an automatic or manual reactor trip. Several event trees in the SPAR model include a top event that represents the nonrecovery of a system-induced initiator. The nominal nonrecovery probabilities used in the base case SPAR model were derived either from operational experience or by applying human reliability analysis. More than one nonrecovery event may be modeled, such as early or late recovery.

Examples of event trees with nonrecovery actions 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.

The initiation event frequency estimates used in SPAR models typically do not include recovery.

Components determined to be failed. This activity involves the treatment of independent failures observed during the operational event. A failure of a structure, system, or component (SSC) is represented in the SPAR model by basic event types based on failure modes (e.g., fail-to-start, fail-to-run, fail-to-open, fail-to-close).

A 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.
Some considerations for modeling a failed SSC include the following:

- A complete failure is modeled by setting the basic event probability of the appropriate failure mode to TRUE.

- For structures, systems or components 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 on failure determination and modeling for details.

- In addition to the modeling the independent failure, the analyst will need to adjust the corresponding common-cause failure event.

- Do not credit an actual observed successful recovery except probabilistically in a recovery analysis (see Step 7, below).

Components determined to be degraded. This activity involves the treatment of a degraded condition observed during the operational event. The degraded condition is represented by basic event types 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 failure probability estimate is usually based on 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:
  - 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 early in the condition duration due to the random nature of the degradation mechanism.

- Reasons for not adjusting the nominal failure probability of a degraded SSC may include
  - Degradation did not reduce the functionality of the SSC and the nature of the failure mechanism would not have reduced functionality early in the condition duration.
  - Degradation did not reduce the functionality of the SSC, but the SSC was declared inoperable, as defined by Technical Specifications.

- Revise probabilities for basic events associated with observed degraded components to the probability of failure given the observed degradation.

- The estimation should consider the following:

---

8 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.
- Probability of proceeding from the observed degraded state to a failed state.
- Chance that the condition would not have been discovered before failure.
- Expected duration of component failure before discovery (standby component).

- For situations in which it is not clear if a component is failed, a detailed engineering analysis or an expert elicitation may be appropriate to provide a best estimate of component status.

- Document engineering factors and bases for judgments that support the best-estimate functionality determination and associated failure probability.

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

- 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).

**Components and human actions that were successful.** This activity involves the treatment of SSC and human actions that were observed during the operational event to have operated or performed successfully. In such cases, the failure probabilities of associated basic events will remain at the nominal failure probabilities.

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 are observed to be accomplished successfully or that are not challenged during the event use a human error probability equal to the nominal human failure probability.

**Potential common-cause failure.** This activity involves the treatment of component failures and degradations with CCF implications that were observed during the operational event. The Common-Cause Plugin Modules in SAPHIRE Version 7 makes the adjustments to the CCF probability based on analyst's inputs to the independent failure basic events.

---

9 A “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.
Inputs can be made using both SAPHIRE Version 7 and GEM. The Alpha Factor Method is used to estimate probabilities for all CCF events in SPAR models.\textsuperscript{10}

Some considerations for modeling CCF include the following:

- The reasons for adjusting the nominal CCF probability of the common cause component group (CCCG) associated with a degraded component may include:
  - Complete failures of all components in a CCCG observed in the operational event.
  - Complete independent failure in only one component in a CCCG observed in the operational event.
  - Complete failure in one component and indications of the same degradation mechanism in one or more components in the CCCG.
  - Similar failures of a like component in different CCCGs across system boundaries.
  - Degradations observed in two or more components in a CCCG, but no failures.

- The probabilities of basic events added to the model to represent CCFs should be estimated using the same CCF database as was used in the development of the SPAR model. Components should be matched as closely as possible to those already included in the database.

- Common-cause failure probabilities used in SPAR models are based "CCF Parameter Estimations, 2003 Update" report. The data collection and analysis methods are based on NUREG/CR-6268, "Common-Cause Failure Database and Analysis System: Event Collection, Classification, and Coding." \textsuperscript{(Ref. 2)}

- Increase the probability for CCF basic event associated with the observed failure. The CCF event adjustment will be performed in SAPHIRE Version 7 based on the following analyst's inputs:
  1. Set basic event for observed failure mode (e.g., failure to start) to TRUE.

\textsuperscript{10} The CCF model used in SPAR model is based on the ratio of independent failure events to CCFs event observed in the operating experience. Since CCFs are infrequent, only a high level, industry average comparisons can be observed in the data. The data shows that the failure of one component in a group of components subject to common-cause failure (i.e., within the same common cause component grouping) implies a greater than normal probability of failure of the remaining components in the CCF group.

This high level comparison can only suggest that the remaining components can fail due to any reason, not necessarily from the same failure mechanism observed in the first component. The SAPHIRE CCF modules adjust the independent failure of the remaining component and the CCF event to collectively represent the condition failure probability given the failure of the first component in the CCCG.

Equipment failures that contribute to CCF events are identified during searches of Licensee Event Reports (LER), Nuclear Plant Reliability Data System (NPRDS) failure reports, and Equipment Performance and Information Exchange (EPIX) failure reports. The results were estimated using the CCF database calculator.
(2a) If CCCG is of size 2, set basic event representing CCF of the unobserved failure mode (e.g., failure to run) to FALSE.

(2b) If CCCG is of size 3 or greater, set basic event representing CCF of the unobserved failure mode to 1.0.

- Assume in general that the potential for CCF impacts exists. The burden of proof for excluding potential CCF impacts (e.g., independent failure) rests with the analyst and should be justified.

**Human error probabilities (HEP).** This activity involves the treatment of deficiencies in operator performance and other potential performance issues that were observed during the operational event. An adjustment may be made to one or more 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.

The adjusted failure probability estimate is based on the SPAR-H Human Reliability Analysis Method documented in NUREG/CR-6883 (Ref. 3). The HEP adjustments are considered in the context in which each operator action occurs; this context is invariably sequence and often cut set specific. The PSF levels for same action in different accident sequences may result in difference in the HEPs.

The PSFs from the SPAR-H Method that are used to estimate HEPs for diagnosis and operator actions include:

- Time available
- Stress
- Complexity
- Experience and training
- Procedures
- Ergonomics and human interface
- Fitness for duty
- Work processes

Some considerations for modeling human action include the following:

- An observed human error is modeled by setting the appropriate basic event probability in SAPHIRE Version 7 or GEM to TRUE.

- An adjustment to an HEP event based on observed performance deficiencies should be performed using the approach documented in SPAR-H Human Reliability Analysis Method (NUREG/CR-6883, Ref. 3).

- Check applications of the SPAR-H Method from previous analyses.

- It is important that the description of the PSFs used by the SPAR-H Method be well understood before applying the worksheets used to estimate an HEP. Request for assistance from a knowledgeable human reliability analyst.
Test and Maintenance Contribution. This activity involves the treatment of a system, train, or component that was disabled for test or maintenance (T/M) activity during the operational event.

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

- Refer to the handbook section on test and maintenance outage modeling for details.
- Treatment of a component in T/M is application specific (refer to the program-specific procedure).

Exposure time (condition duration). The exposure time (sometimes known as failure/condition duration) is used by the SAPHIRE/GEM Version 7 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 Version 7 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 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 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.

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/solution cycles to develop a best estimate of the event significance.

Some considerations for solving the model include the following:

- Nonrecovery event. Set basic events included in the model that represent the recovery of components (individual basic events) 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.

- Truncation value. The runtime associated with a particular analysis is a function of, among other things, the truncation value. 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. A truncation value of 1E-12 typically results in a runtime in the range of a few minutes or less.

- Refer to the plant-specific SPAR model manual, “Notes to Analysts,” for additional details on truncation values.

- If possible for a condition analysis, 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 model are captured in the analysis results.

- Loss of offsite power events often result in significantly longer runtimes that other initiators due to extensive logic associated with emergency diesel generators and their support systems.

- If the event being modeled is not showing up in the minimal cut sets, then the base case model may require re-solution with a lower truncation value. These cut sets may be truncated out in the original base case model results.

- **Condition analysis.** For a condition analysis, the increase in core damage probability ($\Delta$CDP) or “importance” is calculated by first solving the conditional core damage probability (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 Version 7. The importance result is documented in the GEM printout.

- **Overlapping conditions.** For the analysis of overlapping conditions, calculate the importance of each part of the overlap separately, if appropriate for the analysis application (refer to the program-specific procedure). Sum the importance for each part to calculate the overall degraded condition importance (this is performed by the analyst, not automatically by SAPHIRE/GEM Version 7).

- **Initiating event with an observed failure.** Consider the potential impact of failures and unavailabilities observed during an initiating event in a separate condition analysis, if appropriate for the analysis application (refer to the program-specific procedure).

  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.

  - Analyze such a condition if its risk significance is similar to or greater than the risk significance of the initiating event.

  - Report the risk significance (i.e., importance) of such a condition separately from the significance of its associated initiating event.

**Step 6 Review of Initial Analysis 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.
Some considerations for the review of initial results include the following:

- **Analysis inputs.** Check for the proper use of parameter value representing a failure or unavailable basic event (e.g., TRUE vs. 1.0).

- **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 Section 2.8 of Volume 3 of the RASP Handbook for details.

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

- **Cut set reviews.** Using the nominal cut sets from the original and modified base case SPAR models as guides to expected cut set structure, confirm that the results developed from the current case model are consistent with the failures, unavailabilities, and off-normal conditions that were observed during the operational event.
  
  - The probabilities for sequences adversely impacted by the condition or event should be higher in probability than in the base case SPAR model.
  
  - Sequences that were conservatively or simplistically developed in the original model should not exist among the significant 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.
  
  - Basic events impacted by a component failure should not appear in an unmodified form unless this is appropriate for the event. If so, address this in the analysis documentation.
  
  - Components supported by another failed component or train (e.g., a pump supported by an observed failed cooling water train) should have been removed from the dominant cut sets.
  
  - Basic events expected to be contributors to dominant cut sets should be included in those cut sets.
  
  - Basic events that were added or increased in probability to reflect the operational event should be appropriately reflected in the dominant cut sets.
  
  - Investigate any discrepancies in the list of cut sets. Check for “illogical” cut set 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.

- **Multiple operator actions.** Check for multiple operator actions in cut sets to verify that dependencies have been appropriately applied in the human error probabilities.
Appendix 1  Road Map: Risk Analysis of Operational Events

- **Importance measures review.** Using the risk achievement and risk reduction importance measures associated with the conditional cut sets, confirm 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.

- **Another check.** Check that the results are consistent with the failures, unavailabilitys and off-normal conditions that were observed in the operational event and the sequences impacted by the operational event.

- Return to previous analysis steps to resolve any discrepancies.

### Step ☑ Recovery Analysis

Recovery analysis addresses the potential recovery of failed components and human errors prior to core damage. A complete recovery analysis is labor intensive; however, they are usually required for events that are of high risk significance or are controversial.

For some events, a limited recovery analysis may be all that’s needed to address the potential recovery of the failure or unavailability subject to analysis. In some cases, recovery actions are already addressed in the SPAR model, such as

- Event tree top events (e.g., power conversion system recovery)
- Nonrecovery basic events (e.g., restart reactor core isolation cooling, emergency diesel generator recovery)
- Recovery rules (i.e., cut set modifications)
- Recovery analysis (e.g., loss of offsite power recovery)

Recovery analysis provides varying nonrecovery probabilities applied to event tree top events, nonrecovery basic events, and recovery rules.

Some considerations for crediting and applying recovery include the following:

- **More details.** Refer to the handbook section on recovery modeling of failed equipment for details.

- **Solve and review cut sets.** Recover cut sets that constitute at least 99% of the risk.
  - 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.

- **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.

- **As-built, as-operated plant.** Ensure that the current case SPAR model reflects the as-built, as-operated plant for those sequences impacted by the operational event.

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

- **Sequences and cut sets.** Review the final list of significant sequences and cut sets in accordance with the review topics in Step 7.

- **Inputs, assumptions, and 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 7 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, nonrecovery 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 for crediting and applying recovery include the following:

- **Key SPAR model assumptions and technical issues.** Refer to Volume 3 of this handbook, “SPAR Model Reviews,” 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 should be provided of the impact of assumptions that significantly impact the results.

  - If an uncertainty analysis has been performed, address assumptions that result in point estimates outside the 5–95 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 nonrecovery actions added to the initial analysis cut sets, are defined in terms of probability distributions [except basic events assigned a probability of 1.0 (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 the SPAR model parameters can be found in the SAPHIRE Version 7 Training Manuals (Ref. 4).

  - 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 8 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. 1). 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 and current case SPAR model should be linked to the associated assumption.

☐ **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 events tree and fault trees modifications so that they can be independently reproduced (or attach figures).
  
  - Document the revisions and dates of the SPAR model and SAPHIRE/GEM Version 7 code.

☐ **The results.**
  
  - Summarize the results, including the results of sensitivity and uncertainty analyses.
  
  - Attach the SAPHIRE/GEM Version 7 printout, as appropriate.
The references. Reference list 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.
3. References


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 in Table 1.

![Modify Event Window]

Table 1: Process Flag Fields

<table>
<thead>
<tr>
<th>Process Flag</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Success</td>
</tr>
<tr>
<td>W</td>
<td>Failure, Use Fault Tree Logic</td>
</tr>
<tr>
<td>X</td>
<td>Failure, Use Developed Event</td>
</tr>
<tr>
<td>Y</td>
<td>Failure, Use Developed Event</td>
</tr>
</tbody>
</table>

Note: The process flag fields are defined in Table 1.
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.
- 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.
### Table 1. Process Flags

<table>
<thead>
<tr>
<th>Flag</th>
<th>Use on failure branches</th>
<th>Use on success branches</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot; &quot; (a space)</td>
<td><strong>Failure</strong> - Use system logic</td>
<td><strong>Success</strong> - Use the &quot;delete term&quot;</td>
</tr>
<tr>
<td></td>
<td>Use fault tree logic (if available) for the top event. If fault tree logic is not present, then use the developed event probability.</td>
<td>Use the &quot;delete term&quot; process to eliminate failure cut sets based on the event tree success event(s). The &quot;delete term&quot; process looks for, and removes, impossible cut sets from the analysis.</td>
</tr>
<tr>
<td>I</td>
<td><strong>Failure</strong> - Use system logic</td>
<td><strong>Success</strong> - Use the complement of the system logic</td>
</tr>
<tr>
<td></td>
<td>Use fault tree logic (if available) for the top event. If fault tree logic is not present, then use the developed event probability.</td>
<td>Use the complement of the system logic for the successful branch. SAPHIRE Version 7 will then treat the success tree as part of the sequence cut set solving process. Note that (1) this calculation may take a long time and (2) SAPHIRE Version 7 does not perform the Boolean operation $A^<em>B + A^</em>/B = A$.</td>
</tr>
<tr>
<td>W</td>
<td><strong>Failure</strong> - Use system logic</td>
<td><strong>Success</strong> - Use the complement of the developed event</td>
</tr>
<tr>
<td></td>
<td>Use fault tree logic (if available) for the top event. If fault tree logic is not present, then use the developed event probability.</td>
<td>Use the complement of the developed event (i.e., one minus the probability specified for the top event).</td>
</tr>
<tr>
<td>X</td>
<td><strong>Failure</strong> - Use a developed event</td>
<td><strong>Success</strong> - Use the &quot;delete term&quot;</td>
</tr>
<tr>
<td></td>
<td>Use a basic event (named the same as the top event) instead of fault tree logic. The user must specify the failure probability of the top event.</td>
<td>Use the &quot;delete term&quot; process to eliminate failure cut sets based on the event tree success event(s). The &quot;delete term&quot; process looks for, and removes, impossible cut sets from the analysis.</td>
</tr>
<tr>
<td>Y</td>
<td><strong>Failure</strong> - Use a developed event</td>
<td><strong>Success</strong> - Use the complement of the developed event</td>
</tr>
<tr>
<td></td>
<td>Use a basic event (named the same as the top event) instead of fault tree logic. The user must specify the failure probability of the top event.</td>
<td>Use the complement of the developed event (i.e., one minus the probability specified for the top event).</td>
</tr>
</tbody>
</table>