Risk Assessment of Operational Events

Handbook

Volume 1 – Internal Events

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

UNITED STATES NUCLEAR REGULATORY COMMISSION

Revision 3

December 2025

SDP • ASP • MD 8.3

TABLE OF CONTENTS

ACRONYMS

AC	alternating current
AFW	auxiliary feedwater
ANS	American Nuclear Society
AOP	Abnormal operating procedure
ASME	American Society of Mechanical Engineers
ASP	Accident Sequence Precursor (Program)
BOP	balance of plant
BWR	boiling-water reactor
CCCG	common cause component group
CCDP	conditional core damage probability
CCF	common-cause failure
CCW	component cooling water
CDF	core damage frequency
CDP	core damage probability
CFM	cognitive failure mode
DC	direct current
ECA	event and condition assessment
EDG	emergency diesel generator
EFW	emergency feedwater
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
ESW	emergency service water
FIP	final integrated plan (FLEX)
FTC	failure to close
FTO	failure to open
FTR	failure to run
FTS	failure to start
gpm	gallons per minute
HEP	human error probability
HFE	human failure event
HPCI	high-pressure coolant injection
HPCS	high-pressure core spray
HRA	human reliability analysis
IDHEAS-ECA	Integrated Human Event Analysis for Event and Condition Assessment
IMC	Inspection Manual Chapter
INL	Idaho National Laboratory
IRIS	Industry Reporting and Information System
LER	licensee event report

LOCA	loss-of-coolant accident
LOOP	loss of offsite power
LPI	low-pressure injection
MD	management directive
MDP	motor-driven pump
MFW	main feedwater
NOED	notice of enforcement discretion
NPP	nuclear power plant
NPSH	net positive suction head
NRC	U.S. Nuclear Regulatory Commission
PCS	power conversion system
PD	performance deficiency
PIF	performance influencing factor
PORV	power-operated relief valve
PRA	probabilistic risk assessment
PSF	performance shaping factor
PWR	pressurized-water reactor
RADS	Reliability and Availability Data System
RASP	Risk Assessment Standardization Project
RCIC	reactor core isolation cooling
RCP	reactor coolant pump
RCS	reactor coolant system
RG	regulatory guide
RHR	residual heat removal
RIL	research information letter
SAPHIRE	Systems Analysis Programs for Hands-on Integrated Reliability Evaluations
SBO	station blackout
SDP	Significance Determination Process
SPAR (model)	standardized plant analysis risk (model)
SRA	senior reactor analyst
SRV	safety relief valve
SSC	structure, system or component
SSIE	support system initiating event
TDP	turbine-driven pump
T/M	test or maintenance
TS	technical specifications

Internal Events: Introduction	Section 1

1 Introduction

1.1 Objectives

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

The second objective is to provide analysts and standardized plant analysis risk (SPAR) model developers with additional guidance to ensure that the SPAR models used in the risk analysis of operational events represent the as-built, as-operated plant to the extent needed to support the analyses. The individual plant SPAR models represent plant design and operation to a sufficient level for analyses and include the current industry average performance information.

This handbook represents the best practices based on feedback and experience from the analyses of over 900 precursors of events dating back to 1969 in the Accident Sequence Precursor (ASP) Program and numerous Significance Determination Process (SDP) Phase 2 and 3 analyses (now commonly known as detailed risk evaluations) since 2000.

1.2 Scope of the Handbook

1.2.1 Applications

The methods and processes described in the handbook can be primarily applied to event and condition assessments (ECAs) for the SDP, the ASP Program, notice of enforcement discretion (NOED), and Management Directive (MD) 8.3, “NRC Incident Investigation Program,” (ML22294A067). Collectively, these analyses are called ECAs in this handbook. The guidance for the use of SPAR models and Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) software package can be applied in the risk analyses for other regulatory applications, such as the Generic Safety Issues Program and special risk studies of operational experience.

1.2.2 Relationships with 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,” (ML24257A157), MD 8.3, IMC 0308, “Reactor Oversight Process Basis Document,” (ML24269A231) and IMC 0309, “Reactive Inspection Decision Basis for Reactors,” (ML23234A176). It is not the scope of this handbook to repeat program-specific requirements, since these requirements may differ among applications and may change as programs evolve. Program-specific requirements supersede guidance in this handbook.

1.2.3 Deviations from Methods and Guidance

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

1.3 Audience for the Handbook

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

1.4 Handbook Content

The Risk Assessment of Operational Events Handbook consists of this volume (i.e., Volume 1), which covers guidance associated with internal events, and the following three additional volumes:

- Volume 2, "Risk Assessment of Operation Events Handbook—External Events," (ML080300179),
- Volume 3, "Risk Assessment of Operation Events Handbook – SPAR Model Reviews," (ML102850267), and
- Volume 4, "Risk Assessment of Operation Events Handbook – Shutdown Events," (ML111370163).

1.4.1 Volume 1, Internal Events

Volume 1 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 occur at nuclear power plants (NPPs).[1]

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

- Exposure Time Modeling
- Failure Modeling
- Mission Time Modeling
- Common-Cause Failure (CCF) Modeling
- Modeling Recovery and Repair
- Multi-Unit Considerations
- Initiating Event Analyses
- Human Reliability Analysis (HRA)

[1] In this handbook, "initiating event" and "degraded condition" are used to distinguish an incident involving a reactor trip demand versus 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.

- Loss of Offsite Power (LOOP) Events
- Support System Initiating Events (SSIEs)

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

1.4.2 Volume 2, External Events

Volume 2 provides methods and guidance for the risk analysis of initiating events and conditions associated with external events. External events include internal floods, internal fires, seismic hazards, external floods, external fires, high wind, tornadoes, hurricanes, and others. Volume 2 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

1.4.3 Volume 3, SPAR Model Reviews

Volume 3 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. These checklists were based on the NUREG/CR-3485, "PRA Review Manual," (ML20135H483), American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS) RA-Sa-2009, "Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," and Regulatory Guide (RG) 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," (ML20238B871), and experiences and lessons learned from SDP and ASP analyses.

In addition, Volume 3 summarizes key assumptions in a SPAR model and unresolved technical issues that may produce ambiguities in the analysis results. The importance of these assumptions or issues depends on the sequences and cutsets that were impacted by the operational event. Additionally, plant-specific assumptions and issues may play an even larger role in the analysis uncertainties.

1.4.4 Volume 4, Shutdown Events

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

1.5 Future Updates to the Handbook

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

1.6 Questions, Comments, and Suggestions

Questions, comments, and suggestions on Volume 1 of the Risk Assessment of Operational Events Handbook should be directed to the SRAs in the Office of Nuclear Reactor Regulation (NRR) or members of the Group for Risk Evaluation and Assessment Tools Review.

Analysts seeking assistance from the SPAR Model Help Desk, which is contracted by Idaho National Laboratory (INL), should email questions and/or request to SPARModelHelp@inl.gov.

2 Exposure Time Modeling

2.1 Objective and Scope

This section provides guidance for adjusting the baseline exposure time (1 year) in SAPHIRE to best reflect the duration period of the failed or degraded structure, system, or component (SSC). The exposure time (sometimes known as failure or condition duration) is used by the SAPHIRE code in a condition analysis to model the duration over which the risk of the condition (i.e., failure, degradation) is measured. After SAPHIRE completes the cutset evaluation, it will apply the exposure time of the failure or degradation. The estimation of exposure time for various conditions observed is discussed below. This section applies to a condition analysis as part of SDP, ASP, NOED, or MD 8.3 assessments.

2.2 Definitions

2.2.1 Exposure Time[2]

Exposure time (*T*) is the duration period of the failed or degraded SSC being assessed that is reasonably known to have existed.

– The repair time (if applicable) should be included in the exposure time.

– Exposure time may be operating mode (i.e., power level) dependent. For example, periods while a plant is shut down are not included in the exposure time unless the component/system was required by technical specifications (TS) to be operable during shut down.

2.2.2 Repair Time

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

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

– For MD 8.3 assessments, if at the time of the analysis repairs are still ongoing and the plant is still at power, then repair time should not be included in the exposure time.

[2] SAPHIRE uses the term "duration" instead of exposure time.

[3] The ASME/ANS PRA Standard referred in this handbook includes ASME/ANS RA-Sa-2009, as endorsed by RG 1.200.

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

- If the plant is shut down and the deficiency only affects an at-power condition, then repair time while shut down should not be included.
- If the repair involves significant time requiring design and construction activities (e.g., fire wall), and other mitigating actions were immediately taken (e.g., fire watch), then repair time may not be included. This is left to the analyst’s judgment.

2.2.3 t Period

The *t period* is the time between the last successful functional operation and the unsuccessful functional operation or failure discovery date.

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

2.3 Exposure Time = t + Repair Time

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:

- The failure was determined to have occurred when the component was last functionally operated in a test or unplanned demand.
- 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 the last successful operation includes the following:

- The failure occurred due to human error as the component was being secured from the last test or operation.
- A mechanical failure resulting in a failure to start (FTS) that could have only occurred when the component last operated or changed state.
- The replacement part was defective, but it passed the 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.

2.4 Exposure Time = t/2 + Repair Time

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

This exposure time determination approach is appropriate for standby or periodically operated components that fail due to a degradation mechanism that gradually affects the component. The *t/2 period* should be considered for the following reasons:

– 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 identify the inception of the failure, but a failure mechanism and cause were reasonably known.

– A "hard failure" of the SSC occurred in an actual demand or would occur during a hypothetical demand and hence would be modeled by setting the basic event to 1.0 or True in the model. A latent condition which might increase the probability of failure of the SSC (modeled by increasing the basic event failure probability) should not be assessed using *t/2* as this approach already captures the epistemic uncertainty of the degradation mechanism.

Repair time is added to the *t/2 period*. Evidence for considering that the failure occurred sometime between the last successful operation and discovery time includes 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, general service wear, oxidation, or other time-based degradation mechanisms).

2.5 Exposure Time for Component Run Failures

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

2.5.1 Sum of Run Times > PRA Mission Time (24 hours)

The exposure time starts at the time when the component no longer had the capability to operate for the 24-hour PRA mission time. This approach could be conservative if the unknown inception time of the degradation mechanism was after the calculated beginning of the exposure time.

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

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

<table>
<tr><th>Jan</th><th>Feb</th><th>Mar</th><th>Apr</th><th>May</th><th>Jun</th><th>Jul</th><th>Aug</th><th>Sep</th></tr>
<tr><td>4 hours</td><td>4 hours</td><td>4 hours</td><td>4 hours</td><td>4 hours</td><td>4 hours</td><td>4 hours</td><td>4 hours</td><td>4 hours</td></tr>
<tr><td colspan="3">←Inception of condition</td><td colspan="6">Failure to run (FTR) occurs→
← Exposure Time (based on 24-hour PRA mission time)→</td></tr>
</table>

2.5.2 Sum of Run Times < PRA Mission Time (24 hours), Inception Time Known

When the inception of the condition is known and the accumulation of run time between the time of inception and time of failure is less than the PRA mission time (e.g., 24 hours), the exposure time should start at the time of inception and end when the repaired component was returned to service.[6]

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

<table>
<tr><th>Jan</th><th>Feb</th><th>Mar</th><th>Apr</th><th>May</th><th>Jun</th><th>Jul</th><th>Aug</th><th>Sep</th></tr>
<tr><td>1 hour</td><td>1 hour</td><td>1 hour</td><td>1 hour</td><td>1 hour</td><td>1 hour</td><td>1 hour</td><td>1 hour</td><td>1 hour</td></tr>
<tr><td colspan="9">←Inception of condition FTR occurs→
←------------------ Exposure Time (based on 24-hour PRA mission time) ---------------------→</td></tr>
</table>

Repair time should be included in the exposure time for both cases above.

2.6 Exposure Time for Continuous Component Operation Failures

For failure of a component that is normally in continuous operation while at-power (e.g., normally operating service water pump), the exposure time should be the PRA mission time (i.e., 24 hours).[7]

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

2.7 Maximum Exposure Time

The maximum exposure time (*T*) in a condition analysis is usually limited to one year; even though the condition may have existed for longer than one year (e.g., design deficiency present since installation, modification, or construction). If a degraded condition exceeds 1 year, this information should be included in the analysis as a qualitative factor, particularly if a regulatory

[6] For the case where the inception time is not known, the case "Sum of Run Times > PRA mission time (24 hours)" would apply.

[7] If the mission time for the component is less than 24 hours, then that time should be used. If there are epistemic uncertainties on the mission time for the SSC, then the default of 24 hours should be used.

decision is being informed by it.

2.8 Exposure Time for Multiple Conditions

In SDP analyses, the risk significance of multiple conditions is only assessed if concurrent degraded conditions are caused by the same performance deficiency (PD) (except for poor management or similar crosscutting programmatic issues). This category includes the summation of exposure time segments of multiple equipment or functional degradations. The treatment of multiple conditions is specific to the analysis application. Refer to the program-specific procedure (i.e., SDP, ASP, and MD 8.3). Section 2.10 of this handbook provides examples of exposure times for multiple conditions.

2.9 Exposure Time for Test or Maintenance (T/M) Contribution

This category includes the addition of an exposure time segment involving a failed/degraded component and a concurrent unavailability of a component in test or maintenance (T/M) due to an unrelated cause. Concurrent unavailability of components due to T/M is treated differently in ECAs completed as part of the ASP Program and the SDP. Section 2.10 of this handbook provides examples describing how the exposure time for T/M is handled in different analyses.

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 period that the component was tagged out-of-service.

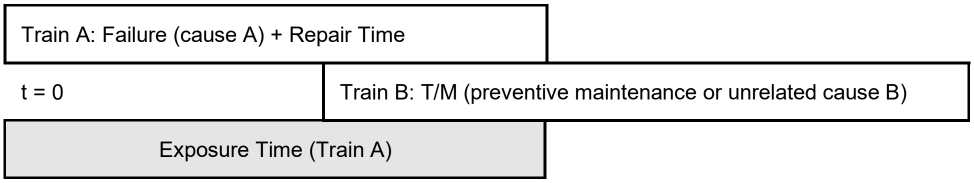
Maintenance performed during shutdown is not included in the determination of component unavailability during power operation. If a scheduled T/M reveals a degraded condition, then the T/M outage time, as well as the repair time, should be included in the exposure time.

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

2.10.1 Case A – Condition Analysis of One Failure

Failure of one train and unavailability of another train with overlapping exposure times:

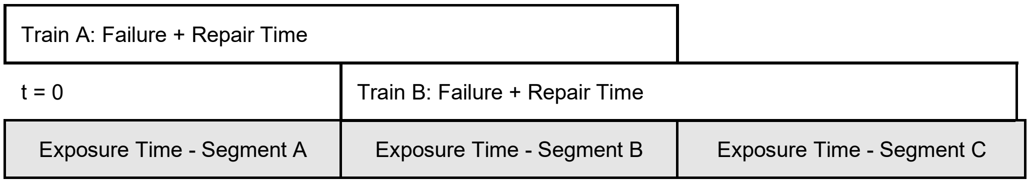
- If the cause of the T/M outage of Train B is not related to the PD that caused the failure of Train A, then the exposure time only applies to the Train A failure.


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

2.10.2 Case B – Condition Analysis of Two Failures with Overlap

Failure of one train and a second failure in another train with overlapping exposure times:

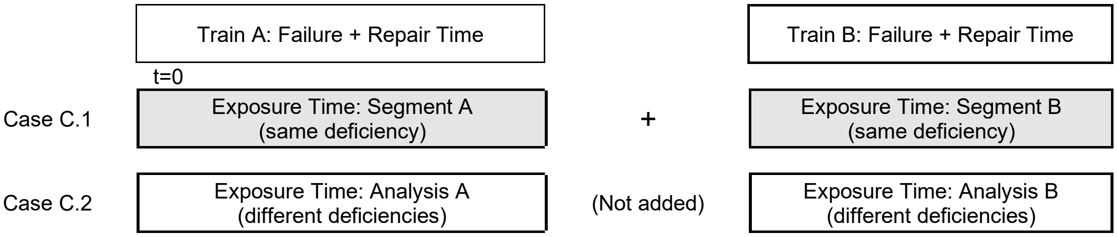
- If both failures were related to the same PD *(*applies to SDP and ASP analyses*)* or if both failures are not related to the same PD *(*applies to ASP analysis only*)*, then the exposure time is the sum of the three segments.


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

2.10.3 Case C – Condition Analysis of Two Failures without Overlap

Failure of one train and a second failure in another train with no overlapping exposure times:

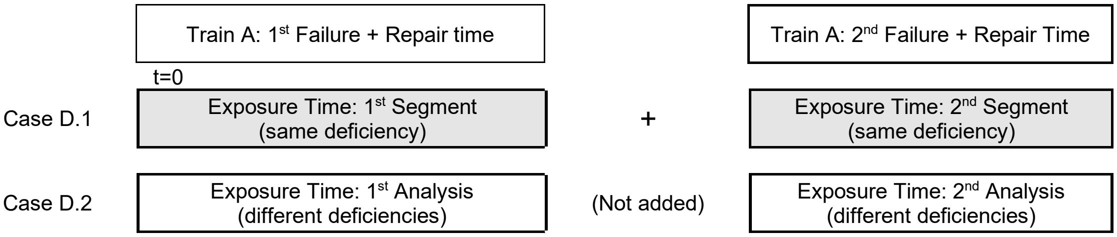
- *Case C.1*. If both failures were related to the same PD (other than poor management or cross-cutting programs), then the exposure time is the sum of the two segments (applies to SDP and ASP analyses*).*
- *Case C.2*. If both failures are not related to the same PD, then each condition is analyzed separately *(*applies to SDP and ASP analyses*).*


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

2.10.4 Case D – Condition Analysis of Repeated Failures in the Same Train

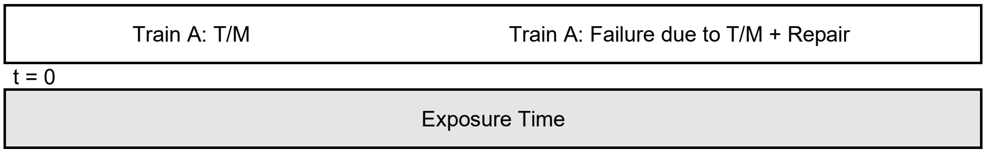
Failure of a train and a second failure of the same train (after attempted repair of the first failure):

- *Case D.1*. If both failures were related to the same PD (other than poor management or cross cutting programs), then the exposure time is the sum of the two segments (applies to SDP and ASP analyses*).*
- *Case D.2*. If both failures are not related to the same PD, then each condition is analyzed separately (applies to SDP and ASP analyses).


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

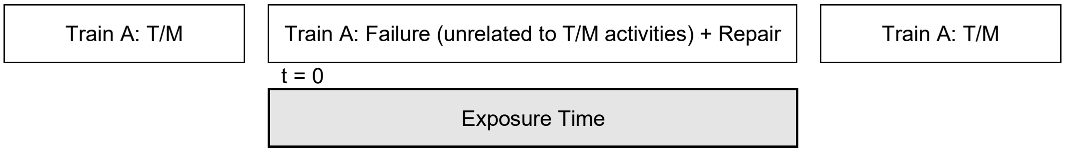
2.10.5 Case E – Failure of a Train Caused by a Prior T/M Activity

If a component was not properly returned to service following a test or maintenance activity, then the exposure time includes the first maintenance outage time.



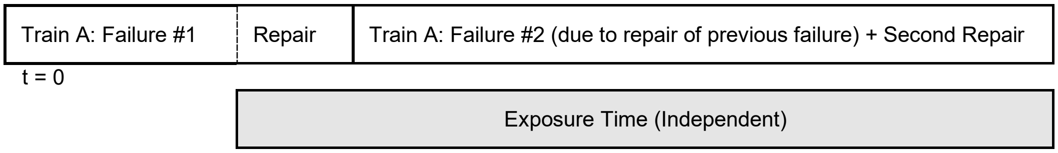
2.10.6 Case F – Failure of a Train not Caused by T/M Activity

T/M outages not related to the failure are not included in the exposure time.



2.10.7 Case G – Repeated Failures in Same Train, Later Failure Induced by Repairs of the First Failure

If the repair of the first failure caused the second failure, then the exposure time of the second failure includes the repair time of the first failure.


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

3 Failure Modeling

3.1 Objective and Scope

This section provides guidance for the treatment of failures observed during an operational event. A failure of an SSC is represented in the SPAR model by basic events based on failure modes (e.g., FTS, FTR, failure to open (FTO), and failure to close (FTC)). The treatment of failures of varying severity in ECA and the modeling of failures in SPAR models using the SAPHIRE code are discussed below. This section applies to ECAs in SDP, ASP, NOED, or MD 8.3 assessments.

3.2 Treatment of Failures in ECA – Types of Failures

Component malfunction events can be classified into one of the following three failure event severity categories as defined in Section 5.2 of NUREG/CR-6823, "Handbook of Parameter Estimation for Probabilistic Risk Assessment," (ML032900131): (1) catastrophic failures, (2) degraded failures, and (3) incipient failures. The treatment of these failure categories in ECA are summarized below. Specific examples in ECA are provided in Section 3.3, below.

3.2.1 Catastrophic Failures

Catastrophic failures require some kind of repair or replacement action on the component to restore functionality. These types of failures are generally modeled by setting the basic event to TRUE and setting its non-recovery probability (if applicable) to TRUE.

3.2.2 Degraded Failures

Degraded failures can prevent a system or train from meeting the success criteria assumed in the PRA model. These types of failures may result in SSCs having a higher failure probability on demand (e.g., FTS) or failing before completing their mission time (e.g., FTR). Degraded structures may fail from a more severe external event or fail at a condition outside its rated specifications (e.g., a fire wall rating).

Degraded failures are generally modeled by one of the following applications:

- Adjusting the failure probability to a higher value, based on appropriate engineering analysis, to reflect increased likelihood of failure (e.g., due to aging, growth of a crack).
- Setting the basic event to its non-recovery probability (based on a recovery analysis) when it is not feasible to conduct an engineering analysis to determine the impact of the degradation on the failure probability.
- Adjusting the PRA success criteria.

  For example, assume that there is a degraded pump in a three-train system with 1 out of 3 success criterion. If degradation reduces the pump's flow rate or head, it may be appropriate to use a 2 out of 3 success criterion to reflect the impact of the pump degradation.

In some cases, refining the SPAR model is necessary to remove conservatism and, therefore, resulting in a reduction in the importance of the degradation.

3.2.3 Incipient Failures

Incipient failures have no significant degradation in performance but there are indications of a developing fault. An incipient failure that does not conform to its safety analysis basis may be classified as inoperable. The term "inoperable" has regulatory significance. It does not necessarily imply a state of physical failure. A component can be inoperable and still able to perform its PRA function over its assumed mission time.

Although an incipient failure will typically lead to a corrective action, the corrective action may or may not make the component unavailable to perform its function.

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

3.2.4 Unknown Classification of Severity

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

3.3 Treatment of Failures in ECA – Examples

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

3.3.1 Catastrophic Failure During Tests

An FTS or FTR 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.

3.3.2 Degradation without Loss of Function (Incipient Failure)

A degraded failure that was not serious enough to prevent the component from performing its function should be treated as an incipient failure. The failure of the component should match the definition of the failure in the PRA model.

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

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

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

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

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

3.3.3 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 and there is no impact on its ability to perform mitigation functions during the PRA mission time.

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

3.3.4 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 Industry Reporting and Information System (IRIS) database for similar spurious failures may reveal a chronic pattern. An update of the component failure probability may be warranted for repeated occurrences of spurious failures. If a spurious failure occurred during an unplanned demand, then the basic event should be set to TRUE. Recovery may be appropriate since spurious failures are in many cases easily recoverable.

3.3.5 Failure that Can Be Easily Recovered

A component failure that can be quickly recovered may be modeled in the PRA as a failure with recovery. Refer to Section 6 for details.

3.3.6 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 SDP analyses, the cause of the failures should be related to the same PD. Refer to Section 2 for details and exceptions.

3.3.7 FTR of a Standby Component

3.3.7.1 Extended Run Failure

A component that FTR during an extended test (e.g., EDG 24-hour duration test) or under normal operation (e.g., motor-driven auxiliary feedwater (AFW) pump during hot shutdown conditions) may not impact the mission time of many sequences modeled in the PRA.

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

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 (SBO) model, if the wear was time dependent and not randomly catastrophic.

3.3.7.2 Short Test Failure

A component that FTR during a routine surveillance test may accumulate enough run time to satisfy the mission time of short-term sequences. A run failure may alternatively signal the presence of a condition that might have precluded success in longer-run-time missions for an appreciable exposure time. Refer to Section 2 for a discussion of this point. A component that FTR may indicate a gradual degradation with longer successful 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 because the degradation was not too advanced. The rate of gradual degradation is often difficult to estimate. The degradation rate could be linear or exponential.

3.3.8 FTR 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 unsuccessful operator intervention may need to be considered (e.g., manual alignment of a standby train).

3.4 SPAR Models – Failure Mode Definitions

3.4.1 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, FTR events for some components may be split into two separate basic events. For example, the EDGs have a basic event for failure to load run within 1 hour and another basic event that represents a failure to run for the remaining 23 hours of the PRA mission time. Whatever definitions are used; the failure event must be matched with the appropriate basic event.

3.4.2 Where to Find Failure Mode Definitions Used in SPAR Models

Failure probabilities used in SPAR models are based on the analysis methods and results from of NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," (ML070650650). The failure modes and component boundary definitions are also documented in Appendix A of NUREG/CR-6928. Updates to NUREG/CR-6928 will be posted on the Reactor Operational Experience Results and Databases Web Page.[9] Modeling limitations that exclude failure modes can be found in the fault tree section in the plant-specific SPAR model manual.

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

3.4.3 FTS Events in SPAR Models

FTS events are typically modeled to occur prior to steady-state operation. There is no explicit time frame (e.g., 30 minutes) associated with FTS.

3.4.4 FTR Events in SPAR Models

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

3.5 SAPHIRE Code – Modeling Failures

3.5.1 Location of Basic Event(s) Used in the SPAR Model

Basic event modification(s) can adversely affect other parts of the SPAR model and, therefore, the analyst needs to know the locations the applicable basic event(s) are used. Specifically, modifications may not be appropriate for all sequences, especially for time-dependent recovery/repair actions.

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

Some considerations include the following:

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

3.5.2 CCF Analysis in Event Assessment

This activity involves the treatment of component failures and degradations and the CCF implications for the evaluation of the operational event. Refer to Section 5 for detailed guidance on this topic.

3.5.3 Consideration of Success Terms in SAPHIRE

SAPHIRE normally uses a quantification method that only considers event tree failure branches. The success branches are not quantified. If adjusting a basic event to a higher probability results in an increase in event tree branch failure probability so that the success branch probability is significantly affected (reduced to something less than 0.95), then the success branch may have a significant impact on the results. Analysts should consult the SPAR Model Help Desk for guidance on incorporating success terms in the model results.

3.5.4 Modeling a Support System Failure

If the support system is not included in the SPAR model, the impact of the failure on front line safety systems is addressed by setting the impacted components to TRUE in ECAs. CCF implications should be reviewed in accordance with Section 5. Section 9.0 provides information on modeling support systems that can cause initiating events. The modeling of a support system failure recognizes that as long as the failure remains unrecovered, all impacted SSCs are unavailable; but if the support system failure is recovered, all impacted SSCs may be recoverable. Use of an event tree may be more appropriate for modeling support system failures when the operating experience data show likelihood of recovery as a function of time after failure.

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

3.5.5 Whether to Set the Basic Event to TRUE or 1.0 in SAPHIRE[10]

The mapping of an observed failure in the SPAR model usually requires the analyst to set the basic event to TRUE in SAPHIRE. Setting the basic event to 1.0 (which also means failed) can result in differences in cutsets. Both choices have advantages and disadvantages.

Basic event(s) of a failed component(s) should be set to TRUE in ECAs to ensure the potential for CCF is properly estimated. In addition, setting the basic events to TRUE results in desired changes to the applicable fault tree logic (e.g., pruning appropriate branches and basic events from the fault tree) and the affected fault trees will be resolved to generate new cutsets rather than just re-quantifying the existing cutsets with a new basic event failure probability. Note that post-processing rules that include basic event(s) that are set to TRUE will not be applied to resulting sequence cutsets if the single pass solve method in SAPHIRE is used. This issue can be mitigated by using the multi pass solve method in SAPHIRE. Basic event(s) of failed component(s) should only be set to 1.0 if a deviation of key CCF principles is identified (see Section 5.8.2 for additional information).

SAPHIRE uses the multi pass solve method as the default selection in the ECA workspace. In most cases, this selection will provide the user with the best results as it mitigates some key issues as discussed in Section 3.5.5.2. However, analysts should carefully review the ECA

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

cutsets to determine if the selection of the single pass solve method may provide more accurate results.

4 Mission Time Modeling

4.1 Objective and Scope

This section provides guidance for adjusting the mission time (i.e., decrease or increase) of an SSC from the baseline 24-hour mission time that is typically credited in SPAR models. The ASME/ANS PRA Standard defines mission time as "*. . . the time period that a system or component is required to operate in order to successfully perform its function.*" In the SPAR models, a 24-hour mission time is assumed for all sequences and most SSCs. The supporting requirements in the ASME/ANS PRA Standard suggest a minimum mission time of 24 hours. However, exceptions are permitted for shorter and longer mission times for certain situations, as discussed below. Considerations for adjusting mission times in SPAR models for ECA using the SAPHIRE code are also discussed. This section applies to ECAs in SDP, ASP, NOED, or MD 8.3 assessments.

4.2 Treatment of Mission Time in ECA – General Considerations

The SPAR models assume a PRA mission time of 24 hours for all sequences and components. Use of mission times other than the full PRA mission time should be rare and should follow the supporting requirements from the ASME/ANS PRA Standard. A component's mission time is typically 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, analysts should contact the SPAR Model Help Desk before or after making the model modification. Checklists to guide the review of SPAR model modifications are provided in Volume 3 of this handbook. These considerations apply to individual basic events and may also apply to classes of basic events sharing the same mission time requirement.

4.3 Decreasing Mission Time (< 24 Hours)

Component mission times less than 24 hours may be appropriate for certain sequences. Specifically, mission times for individual components that function during the accident sequence may be less than 24 hours if the component is not required for the complete PRA mission time. Considerations for decreasing the mission time of a component may include:

- Component mission times may be sequence or cutset dependent.
- Decreasing the mission time of a component is more important for those with a higher FTR probability.

  For example, turbine-driven pumps (TDPs) have a higher failure rate than motor-driven pumps (MDPs), 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 component mission time that is normally secured early in the sequence as the result of the successful use of an alternate system that is modeled at the later part of the sequence. However, taking credit for an alternate system would need to be validated with licensee emergency operating procedures (EOPs), reviews of

training documents, etc.

- The SPAR models convolve the EDG FTR distributions on applicable SBO cutsets to eliminate the simplifying assumption that all EDG FTR occur at T_0. The convolution adjustment factors in SPAR model are provided in time-dependent basic events (e.g., 30 minutes, 1 hour, 2 hours, etc.) for EDG FTR and non-recovery of offsite power. Note that some licensee PRAs use a mission time less than the PRA mission time of 24 hours for the EDGs during applicable LOOP and/or SBO accident sequences to address this issue. It is not appropriate to use both the convolution adjustment factors and a reduced mission time.

4.4 Increasing Mission Time (> 24 Hours)

Although there are hazards (e.g., seismic, high winds, etc.) that could potentially result in NPPs relying on safety-related SSCs (e.g., EDGs, AFW, RCIC/HPCI, etc.) to function well beyond the PRA mission time of 24 hours before balance-of-plant (BOP) systems can be restored, it the current state of practice to keep the mission at 24 hours for these scenarios given a safe/stable end state has been reached.

4.5 Revising Mission Times

The method used to revise the mission time of applicable component(s) will depend on whether the change is applicable to single component or multiple, redundant components within the same system and whether the change is applicable to the entire model or only to certain accident sequence(s) or cutset(s). The following subsections provide an overview of the methods typically used to modify the mission times of component(s) within the SPAR models. Analysts should contact the SPAR Model Help Desk for assistance in revising mission times.

4.5.1.1 Revising Multiple, Redundant Component Mission Times for All Accident Sequences

To revise the mission times to multiple, redundant components for all accident sequences, analysts should modify mission time of the applicable FTR template event in SAPHIRE. Modifying the mission time of the FTR template event will change mission time for all components that use that template event. However, analysts must ensure that the revised template event is not used for components whose mission time should not be adjusted. Note that there are two FTR template events for most components. An early FTRFR template event covers the first hour of operation, while a late FTR template event covers the remaining 23 hours of operation. Unless the mission time is being reduced to 1 hour or less, analysts only need to modify the late FTR template event.

4.5.1.2 Revising Single Component Mission Time for All Accident Sequences

To revise the mission time of a single component for all accident sequences, analysts need to modify mission time of the applicable FTR basic event in SAPHIRE. However, this modification cannot be done directly since the FTR basic events are compound events that use both early and late FTR template events. If the applicable FTR template events are only used for the applicable component, then the analyst can change the applicable FTR template event. However, if the applicable FTR template events are used for multiple components, analysts must create new FTR templates for the applicable component. The mission time of the new template events can then be changed to achieve the desired result.

4.5.1.3 Revising Mission Time(s) for Applicable Accident Sequences

The revision of a mission time of either multiple, redundant components or a single component for a single or limited set of accident sequences requires a new system/function fault tree to be created. This new system fault tree will include the FTR basic event with revised mission times using the guidance provided in the previous subsections. Analysts can then replace the original system/function fault tree with this new fault tree by either direct substitution or creating new event tree linkage rules. This process will allow the unaffected accident sequences to use the original fault trees with the unchanged mission times.

4.5.1.4 Revising Mission Time(s) for Applicable Cutsets

If a mission time change for either multiple, redundant components or a single component for a single or limited set of cutsets is needed, new FTR basic events need to be created. Analysts will then adjust the mission times of these new basic events using the guidance provided in the previous subsections. Post-processing rules can then be created to substitute the original basic event(s) for the new basic event(s).

5 CCF Modeling

5.1 Objective and Scope

This section provides background information on the CCF modeling in the SPAR models, including the supporting parameter estimations, and guidance on how the potential for CCF is treated in ECAs. In addition, guidance is provided on identifying and evaluating the key uncertainties associated base SPAR CCF modeling and treatment of potential CCF within ECAs. This section applies to ECAs in SDP, ASP, NOED, and MD 8.3 assessments.

5.2 CCF Models

The ASME/ANS PRA Standard lists the four models for estimating CCF parameters (Capability Categories II and III)— (a) Alpha Factor Model, (b) Basic Parameter Model, (c) Multiple Greek Letter Model, and (d) Binomial Failure Rate Model.[11] In addition, the Beta Factor approach is referenced under Capability Category I. The NRC SPAR models use the Alpha Factor Model. Licensee PRAs typically use either the Multiple Greek Letter Model or Alpha Factor Model. A brief introduction to these two CCF models, along with the Beta Factor Model, is provided below. Additional information on the Basic Parameter Model and Binomial Failure Rate Model is provided in NUREG/CR-5485, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment," (ML20198E585).

5.2.1 Alpha Factor Model

Alpha Factor Model is one of the most utilized CCF models in PRAs, including the SPAR model, because of the ability to calculate its parameters (i.e., alpha factors) directly from the CCF event data. The Alpha Factor Model is a failure event ratio model that uses a set of alpha factors to represent the probability of failure for a specified number of components at the same time due to a shared cause. Each alpha factor, α_k, is the conditional probability that given a failure event within a common cause component group (CCCG) of size m, it will fail exactly *k* components out of *m* components. For example, given a failure event within the CCCG, α_2 is the conditional probability that exactly two items fail at the same time, α_3 is the conditional probability that exactly three items fail at the same time. With $n_k$being the number of failure events involving exactly *k* components failing within a CCCG of size *m*, $\alpha_k$can be calculated as:

$$\alpha_k = \frac{n_k}{\sum_{j=1}^{m} n_j}$$

If $Q_k^{(m)}$ is used to represent the probability of a common cause event involving k specific components in a CCCG of size m (1≤k≤m) assuming a staggered testing scheme, which is represented by the following equation:

[11] See Table 2-2.6-5(d), Supporting Requirements for HLR-DA-D, Index Numbers DA-D5 and DA-D6.

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t$$

For example, the failure frequencies for a three-component system are:

$$Q_1^{(3)} = \alpha_1 Q_t$$

$$Q_2^{(3)} = \frac{1}{2} \alpha_2 Q_t$$

$$Q_3^{(3)} = \alpha_3 Q_t$$

If the system success criterion requires at least 1 of 3 redundant components to function, the system unreliability can be written as:

$$Q_S = (\alpha_1 Q_t)^3 + \frac{3}{2}(\alpha_1 Q_t)(\alpha_2 Q_t) + \alpha_3 Q_t$$

Where the CCF portion of the system unreliability is:

$$Q_{CCF} = \frac{3}{2}(\alpha_1 Q_t)\,(\alpha_2 Q_t) + \alpha_3 Q_t$$

5.2.2 Beta Factor Model

The Beta Factor Model assumes that when a CCF occurs, all components belonging to the CCCG fail simultaneously by a common cause. The Beta Factor Model only distinguishes between individual failure events and CCF of the entire group while ignoring all other combinations.

$$Q_t = Q_I + Q_C = (1 - \beta)Q_t + \beta Q_t$$

The Beta Factor Model is not typically used in licensee PRAs having been replaced by the Multiple Greek Letter Model.[12] However, the Beta Factor Model may be beneficial for use in applications when CCF information is limited or unavailable, or when a more simplified approach is appropriate.

5.2.3 Multiple Greek Letter Model

The Multiple Greek Letter Model is a generalization of the Beta Factor Model. The Beta Factor Model distinguishes only between individual failure events and CCF of entire group by ignoring all other combinations. The Multiple Greek Letter Model considers all independent and common cause contributions to the component failure. Specifically, the Multiple Greek Letter Model parameters consist of the total component failure frequency Q_t (which accounts for all independent and common cause events), and a set of failure fractions that are used to quantify the conditional probabilities of the possible ways the CCF of a component can be shared with

[12] The Multiple Greek Letter Model uses the same parameters as the Beta Factor Model for CCCG sizes of two.

other components in the same group given a component failure has occurred. The following are the Multiple Greek Letter parameters for a CCCG size of three:

- β = conditional probability that the cause of a component failure will be shared by one or more additional components, given that a specific component has failed.

$$\beta^{(3)} = \frac{2Q_2^{(3)} + Q_3^{(3)}}{Q_1^{(3)} + 2Q_2^{(3)} + Q_3^{(3)}}$$

- γ = conditional probability that the cause of a component failure that is shared by one or more components will be shared by two or more additional components, given that two specific components have failed.

$$\gamma^{(3)} = \frac{Q_3^{(3)}}{2Q_2^{(3)} + Q_3^{(3)}}$$

For a CCCG of size three, the failure frequencies under the Multiple Greek Letter Model can be expressed as:

$$Q_1^{(3)} = (1 - \beta)Q_t$$

$$Q_2^{(3)} = \frac{1}{2}\beta(1 - \gamma)Q_t$$

$$Q_3^{(3)} = \beta\gamma Q_t$$

The system unreliability (again assuming the system success criterion requires 1 of 3 redundant components to function) can be written as:

$$Q_S = ((1 - \beta)Q_t)^3 + \frac{3}{2}((1 - \beta)Q_t)(\beta(1 - \gamma)Q_t) + \beta\gamma Q_t$$

It is difficult to derive the Multiple Greek Letter parameters directly and, therefore, these parameters are calculated using the alpha factors using conversion formulae provided in Tables A-2 through A-4 of NUREG/CR-5485. The periodically updated CCF parameter estimation report (the latest one being INL/EXT-21-62940, “CCF Parameter Estimations, 2020 Update,”) provides the estimates for alpha factor distributions as well as those for Multiple Greek Letter parameters.

5.3 CCCG Modeling

A key step in the modeling of CCFs in the SPAR models is the identification of the CCCGs. According to NUREG/CR-5485, a CCCG is *a group of (usually similar [in mission, manufacturer, maintenance, environment, etc.]) components that are considered to have a high potential for failure due to the same cause or causes*. There are three main ways CCCGs are reflected in the SPAR models:

- The most common approach is identifying CCCGs in the SPAR models that are limited to redundant components within the same system. For example, the suction and discharge check valves to redundant pumps are divided into two separate CCCGs (one for the discharge valves and one for the suction valves).

- In some cases, CCCGs may be expanded to contain components with similar, but not fully redundant, functions within the same system. This is usually based on a review of licensee PRAs and benchmarking efforts. For example, there is a CCCG that relates to the potential for CCF of AFW pump volutes regardless of the pump driver (e.g., motor, turbine, or engine).[13]
- The third case expands the CCCGs to include cross-unit components (e.g., cross-unit EDGs when they have the capability to be crosstied).

The most common CCCG practice of only modeling functionally redundant components within the same system is the result of data limitations (i.e., data is collected consistent with this approach). In addition, intersystem CCCGs that contain similar components across multiple systems are generally not used because this would greatly increase the size of the CCCG resulting in challenges in modeling specific system level impacts and larger uncertainties associated due to the lack of operating experience data for large CCCGs.

The ASME/ANS PRA Standard requires PRA model developers to define CCCGs considering the following coupling factors—(a) service conditions, (b) environment, (c) design or manufacturer, and (d) maintenance. However, there is no current guidance on how these coupling factors should be considered when assigning redundant components to a CCCG. For example, no guidance is provided on the circumstances under which similar components, that would typically be in the same CCCG due to sharing several coupling factors, be separated from the CCCG due to having different manufacturers. In addition, the SPAR model developers do not have access to all the required plant information to make a detailed evaluation. Therefore, the current CCCGs in the SPAR models are based on the developers' experience and expectation, along with any available licensee PRA information.

The desire to avoid underestimating CCF impacts has resulted in some SPAR models having redundant components that are associated with multiple, overlapping CCCGs. This can result in an overestimation of the potential CCF. When they appear, these duplicative CCCGs are mostly limited to EDGs and service water pumps.

5.3.1 Guidance on CCCG Modeling

The following subsections provide CCCG modeling approaches for single-unit sites, multi-unit sites with systems that can be crosstied between units, and similar subcomponents of diverse equipment. SPAR model developers will use this approach to modify the SPAR model CCCGs as part of the normal model update process. If the same component is included in multiple CCCGs in a manner not consistent with this guidance, analysts should contact the SPAR Model Help Desk for assistance in modifying the applicable CCCGs to support ECAs on as needed basis.

5.3.1.1 CCCG Modeling for Single-Unit Sites

The CCCG modeling approach is relatively straightforward for single-unit sites. Specifically, functionally redundant components should only be contained in a single CCCG. The existing SPAR models currently follow this approach in most cases. However, there are few exceptions with the most notable exception being that some plants have multiple CCCGs for the EDGs.

[13] In this context, the term pump "volute" includes all hydraulic and supporting components for the pump assembly. This includes the volute casing, the impeller, shaft, bearings, packing, and associated subcomponents.

These duplicative CCCGs typically stem from having EDGs that differ in manufacturer or design and/or having alternative diesel generator(s) (e.g., SBO diesel generator).

The CCCG modeling approach should include redundant components in the same CCCG if the same individual component failure data is used. Component failure data is pooled for components that are determined to be sufficiently similar and, therefore, have the same reliability. For example, the existing EDG failure data is pooled from multiple class 1E EDG manufacturers (e.g., Fairbanks Morse, Worthington, General Motors, etc.). This approach is potentially conservative if the redundant components have a significantly different design because the design CCF coupling factor could be mitigated.[14] However, the redundant components will likely share the other CCF coupling factors (e.g., similar environment, common maintenance practices, etc.). Therefore, the existing practice of grouping these components in the same CCCG in most cases is justifiable. However, this could be a key modeling uncertainty in some ECAs, which can be evaluated using sensitivity calculations.

The existing state-of-practice CCF models (including the Alpha Factor Model) assume that all components withing the CCCG have the same reliability (i.e., the same Q_t). Therefore, if redundant components are judged to be sufficiently different to warrant the use of different individual component failure data, the applicable components should generally not be included in the same CCCG.[15] For example, the basic events representing the different failure modes (e.g., FTS, FTR, etc.) for SBO diesel generators may use different individual component failure data than the EDGs. The use of the different data sets for the EDGs and SBO diesel generators is due to these components being sufficiently different (i.e., significantly diverse) and, therefore, having different reliabilities. Therefore, the SPAR models should not generally include both SBO and Class 1E diesel generators in the same CCCG. However, a plant (or site) that has multiple SBO diesel generators should have a separate CCCG for these diesel generators.[16] Note that this approach is nonconservative since it is expected that some CCF coupling factors (e.g., similar maintenance practices, environments, etc.) will exist between the different diesel generator types. This could be a key modeling uncertainty in some ECAs, which should be evaluated qualitatively and/or quantitatively. However, there are some sites where the SBO diesel generator(s) are similar to the EDGs and grouping them together in a CCCG is appropriate.

5.3.1.2 CCCG Modeling for Multi-Unit Sites with Systems That Can Be Crosstied Between Units

In addition to the single-unit CCCGs of redundant components with the same system per unit, the potential for cross-unit CCF between redundant components across systems/components or systems that can be crosstied between units should be considered. Some SPAR models for multi-unit sites have additional CCCGs for EDGs and/or service water pumps when these components can be aligned/crosstied to multiple units. These additional CCCGs can result in an overestimation of the potential CCF because they are duplicative of the single unit CCF events. However, these overcounting effects will be reduced by using adjusted cross-unit CCF

[14] A different manufacturer does not necessarily constitute a different design.

[15] For ECAs where the reliability of a single component within a CCCG is adjusted to account for an observed degraded condition, the affected component should not be removed from the CCCG.

[16] There are currently no CCF parameters for SBO diesel generators. The generic demand and rate CCF parameters should be used. Future development of SBO diesel generator CCF parameters will be considered.

parameters (see Section 5.4.1 for additional information). If the redundant cross-unit components are judged to be sufficiently different to warrant the use of different individual component failure data (e.g., EDGs and SBO diesel generators), the applicable components should not be included in the cross-unit CCCG.

5.3.1.3 CCCG Modeling of Similar Subcomponents of Diverse Equipment

Some existing SPAR models for PWRs have a CCCG associated with the AFW pump volutes regardless of the types of pump driver (e.g., motor, turbine, and engine). This CCF basic event can have a significant impact on some ECAs because it reduces the risk benefits of having diverse equipment. Operating experience does indicate that there is potential CCF between similar subcomponents of redundant, but diverse, equipment. Specifically, a CCF event occurred in 1998 due to failures of pump packing of both the motor- and turbine-driven AFW pumps at Sequoyah). This CCF event is only included in the generic CCF prior, which includes all CCF events that occurred during the 1997–2015 period. There are no CCF events associated with AFW pump volutes that affected diverse pumps during the rolling 15-year period (2006–2020) used for the Bayesian update.[17]

The modeling of similar subcomponents of diverse redundant equipment goes beyond the standard practice of modeling components per their boundary definitions provided in Appendix A of NUREG/CR-6928 and, therefore, it is not recommended to model this type of potential CCFs explicitly. This does not mean that some CCF coupling factors are not present between redundant, but diverse, components. However, the application of the existing CCF models with the very limited CCF data likely provide results that have greater uncertainties than the benefit their inclusion provides. There is potential for underestimating the risk contribution from CCF of the similar sub-components and this should be treated as an uncertainty in the evaluation.

5.4 Intersystem and Cross-Unit CCF Modeling

As previously stated, the modeling of CCFs in the SPAR models is typically limited to functionally redundant components within the same reactor plant unit and system. However, it is also recognized that similar components across plant units at multi-unit sites (cross-unit) or across different systems within the same unit (intersystem) can share CCF coupling factors such as:

- Hardware similarities (e.g., manufacturer, components)
- Design
- Maintenance practices
- Operational practices
- Environmental factors

This SPAR modeling limitation on cross-unit or intersystem CCF is largely due to how the existing failure data is coded into the CCF database. Failure data is submitted by licensees to Institute of Nuclear Power Operations (INPO) for inclusion in IRIS. INL reviews this failure data, along with LERs, to identify CCF events. The CCF events are coded on a per unit and

[17] The current CCF parameters use the CCF data from the 2006–2020 period. See INL/EXT-21-62940 for additional information.

component basis. However, potential cross-unit and intersystem CCF events can be inferred by comparing failure reports across systems and units; but there are larger uncertainties regarding the strength of the CCF coupling for similar components across systems or units. In addition, the modeling of intersystem CCF would result in CCCGs that become too large and complex to be practical for use using the existing CCF models (e.g., Alpha Factor, Multiple Greek Letter).[18]

One exception to this CCF modeling approach is that some SPAR models (for multi-unit sites) include cross-unit CCF modeling of EDGs and service water pumps.[19] This cross-unit CCF modeling has been the dominant risk contributor in some ECAs. The inclusion of this cross-unit CCF modeling mitigates the potential to provide excessive credit for cross-unit accident mitigation (since cross-unit components may share similar coupling factors with the other unit); however, there is concern that the extension of the existing CCF parameters (i.e., alpha factors) to address cross-unit CCF can overestimate the CCF coupling and result in an overestimation of the risk impact. In addition, this cross-unit modeling can result in additional CCCGs that may double-count the CCF impact (i.e., if the same basic events are included in multiple CCCGs).

5.4.1 Interim Approach for Cross-Unit CCF

A review of the CCF database results in a total of 341 CCF events that occurred from 1989 through 2021. A preliminary review of this data revealed that only 10 percent of these CCF events are associated with similar components across units. Further consideration of SSCs that provide redundant cross-unit functions (e.g., service water, electrical power) indicated that approximately less than 10 percent of the CCF events associated with these SSCs involved cross-unit impacts. Although this was a preliminary review and there are limitations to this data review, this provides indication that the cross-unit CCF coupling is weaker than CCF of redundant components in the same system within a single unit. Therefore, the current SPAR models of record (as of January 2025) that include an extension of the CCCG across units using the existing Alpha Factor Model CCF parameters overestimate the risk impact from potential cross-unit CCF. In some cases, this overestimation could be significant. Additional information regarding the preliminary data review performed to identify existing cross-unit CCF events is provided in “CCCG Modeling and Treatment of Cross-Unit CCFs,” (ML25105A198).

Additional research is needed to calculate cross-unit CCF parameters that can be used to replace the existing CCF parameters in the cross-unit CCF basic events that are currently included in the base SPAR models; however, an interim approach should be used for treating cross-unit CCF in ECAs until cross-unit CCF parameters can be developed.[20,21] To provide a better estimate of the potential for cross-unit CCF in ECAs until cross-unit CCF parameters are

[18] Intersystem CCF is not currently modeled in the SPAR models, which is a nonconservative approach to CCF. Therefore, consideration for addressing the impact of similar components used in multiple systems should be evaluated when an issue impacts similar components found in multiple systems (e.g., motor-operated valves, breakers, fuse holders, fans, etc.).

[19] Some plants have additional crosstie capabilities that are not currently included in the applicable SPAR models. These crossties, including the potential for cross-unit CCF of key components, will be added to the applicable SPAR models if the appropriate plant information becomes available.

[20] In January 2025, the NRC initiated a research task to review existing CCF events to identify cross-unit CCF events. In addition, cross-unit CCF parameters will be calculated for limited set of key components (e.g., EDGs, service water pumps, and circulating water/service water strainers).

[21] This interim approach should not be used on redundant components in individual systems that are shared across multiple units.

available, the best estimate evaluation should use cross-unit CCF parameters that are multiplied by a factor of 0.1.[22] This factor is believed to bound cross-unit CCF for most of the component types and failure modes.[23] These adjustments will also reduce the effect of overcounting effects resulting from having redundant components, such as EDGs, in multiple CCCGs.

Although these adjustments are judged to be the best estimate given the current CCF data and modeling, they should be identified as key uncertainty associated with ECAs. It is recommended that analysts perform sensitivity calculations to bound the effects of the potential for cross-unit CCF. Analysts should contact the SPAR Model Help Desk for assistance in making the adjustments to the cross-unit CCF parameters.

5.5 SSIE CCF Modeling

The SSIE fault trees included in the SPAR models (see Section 11 for additional information) include CCF of the components that could result in a total loss of a support system (e.g., service water, component cooling water (CCW), etc.). The CCF modeling in SSIE fault trees is limited to redundant components (e.g., pumps, heat exchangers, traveling screens, etc.) whose failure within the same PRA mission time (i.e., 24 hours) would result in a complete system failure. In addition, there may be additional CCF terms for some components that are more susceptible to environmental impacts (e.g., traveling screens failing due to sea grass intrusion). The CCF basic events included in the SPAR model SSIE fault trees are either initiating event type failures that are frequency based (with units of per reactor critical year) or failures of standby equipment that are included in the mitigation system fault tree logic.[24]

5.6 CCF Parameter Estimates

The existing CCF parameters (i.e., alpha factors) used in the base SPAR models and potential alternatives for use in both base modeling and/or ECAs are described in the following subsections.

5.6.1 CCF Parameters using Single Generic CCF Prior

The CCF parameters from the 2020 CCF parameter update that are used in the SPAR models are derived using a single generic prior that includes all CCF events from all components, failure modes, and causes. The CCF data set used to develop the single generic prior currently covers the 1997–2015 period. The alpha factors for each applicable component and failure mode type were then calculated for the most recent 2020 CCF parameter update via a Bayesian update using CCF data from 2006–2020. This CCF parameter update is documented in INL/EXT-21-62940, which along with past CCF parameter updates, is provided on the Reactor Operational Experience Results and Databases CCF Web Page. Since different component types and different failure causes could lead to drastically different alpha factors, the above usage of a

[22] No adjustments are made on α_1 (i.e., it will remain at its nominal value).

[23] Possible exceptions include failure of battery chargers to operate and bypass events for circulating water/service water strainers. Note that cross unit components should only be grouped in a cross-unit CCCG when the safety function of interest can be provided by redundant SSCs across multiple units.

[24] The failure mode (e.g. FTS, FTR, etc.) of the CCF basic events for standby equipment will depend on the number of redundant components and success criteria. For systems with more than three trains, all the possible CCF combinations may not be included in the SSIE FT due to limits of the fault tree structure. In these cases, most these unmodeled CCF combinations would be in cutsets that are truncated.

single generic prior could result in significant uncertainty (both under- and over-estimation) in the CCF parameter estimates.

5.6.2 CCF Parameters using Component-Specific Priors

Given the uncertainties associated with using a single generic CCF prior in estimated the existing CCF parameters, prior distributions were derived for five component categories—(1) pumps, (2) valves, (3) strainers, (4) EDGs, and (5) other equipment (e.g., transformers, breakers, fans, heat exchangers, etc.). The CCF data set used to develop these priors covers the same date range as the generic prior (1997–2015). A new set of alpha factors for each applicable component and failure mode type are then calculated via a Bayesian update using the latest 15-year period of CCF data. Note that the prior for the "other equipment" category has similar limitations as the previously used generic prior in that it combines different component types and failure modes. However, the uncertainty impact is expected to be reduced by separating out the other four component types from the prior data. See INL/EXT-21-65527, "Developing Component-Specific Prior Distributions for Common Cause Failure Alpha Factors," Revision 2, for additional information.

The component-specific prior distributions do not eliminate the effects of dissimilar components and/or failure modes have on the alpha factors, but these unwanted effects are reduced. Given this consideration, the NRC is planning to use the component-specific CCF priors (instead of the single generic CCF prior) to calculate the CCF parameters in the next periodic data update; currently planned for 2026. These revised CCF parameters will then replace the existing parameters used in the SPAR models.

Until the CCF parameters are revised in the SPAR models, it is recommended that analysts replace the existing CCF parameters with those calculated using the component-specific priors in all ECAs where CCF is a significant contributor. The revised CCF parameters derived from the component-specific priors (including comparisons with the existing CCF parameters used in the SPAR model) are provided on the publicly available Reactor Operational Experience Results and Databases Web Page. Analysts should contact the SPAR Model Help Desk if assistance is needed in revising the CCF parameters to support ECAs.

5.6.3 Causal Alpha Factors

Both the current CCF parameters and revised CCF parameters using the component-specific prior include CCF data from all causes. However, there has been an interest in developing methods that better focus on the CCF potential in ECAs at the causal level, especially for evaluations performed as part of the SDP. The purpose of SDP risk evaluations is to determine the risk significance of an identified PD at the proximate cause level (see IMC 0308, Attachment 3, "Technical Basis For Significance Determination Process," (ML24257A172) for additional information). Research activities have been conducted to evaluate methods for developing and implementing a causal alpha factor model that may better represent the impact of a specific PD on CCF potential. Although preliminary causal alpha factors have been developed, this approach relies on prior distribution information that introduces uncertainties associated with the use of CCF data from dissimilar components and failure modes. In addition, at the current time, causal CCF methods have some additional implementation challenges associated with mapping PDs to available failure categories and ensuring CCF potential is adequately represented in the causal modeling.

Table 5-1, originally provided in "CCF Work Summary and Conclusions," (ML21055A027), shows the existing failure cause groups used in the CCF Database are not optimal when considering SDP risk evaluations of licensee PDs, apart from those resulting from design issues.[25] Many of the existing failure cause groups can be mapped to multiple PD categories and vice versa. For example, failures from the component cause group associated with setpoint drift may be due to the failure to perform timely preventative maintenance while aging or wear failures may be due to poor design or operational practices. Therefore, it can be challenging to map CCF causes to a single PD category, making implementation of the causal alpha factor modeling challenging and increasing the uncertainties associated with the results.

It should also be noted that the causal alpha factors are based on observed failure data and therefore are conditioned on the existence of an observed failure. Because of this limitation, these parameters do not directly represent the impact of a PD on CCF coupling. Although the strength of the calculated causal alpha factors is correlated to how often the associated cause group appears given a failure event, these parameters do not directly represent the likelihood of a failure (including a CCF event) given the existence of a specific PD. For example, a design issue that has a very strong CCF coupling factor but has rarely occurred in the failure data would have causal alpha factors that represent weaker CCF coupling than might be expected should the design issue occur. As such, the existing failure data also may not reflect the CCF coupling strength for certain causal factors.

Table 5-1. Typical Licensee PD Categories for Existing CCF Cause Groups

CCF Cause Group	Failure Cause	Typical Licensee Performance Deficiency Categories
Component	Internal to component; piece-part	
	Setpoint drift	
	Age or wear	
Design	Construction installation error or inadequacy	Design and Engineering
	Design error or inadequacy	
	Manufacturing error or inadequacy	
Environment	Ambient environmental stress	
	Extreme environmental stress	
	Internal environment	
Human	Accidental human action	Corrective Action Program Maintenance Management Oversight Operations Procedures
	Inadequate maintenance	
	Human action procedure	
	Inadequate procedure	
Other/Unknown	State of other component	
	Other	

Given these limitations, the causal alpha factors are unlikely to provide the best estimate of the potential CCF in ECAs and their use in ECAs is generally not recommended. The CCF parameters derived from component-specific priors reflect the best state of practice approaches

[25] These failure cause groups are those used the CCF data collection, classification, and coding process. Using alternative failure cause groups is not possible without a reevaluation of all applicable CCF data. See NUREG/CR-6268, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding,” (ML072970404).

and should be used. However, the causal alpha factors can be used in sensitivity calculations in certain limited cases. Prior to the use of the causal alpha factor parameters, staff should consult with RES and the SPAR Model Help Desk for assistance in the selection of the appropriate causal alpha factors and appropriate procedures for their use. Additional information on the causal alpha factors is provided in INL/RPT-23-72728, “Causal CCF Parameter Estimations 2020”.

5.7 SPAR Model R-Type CCF Events

Most CCF basic events in the SPAR models use the SAPHIRE R-type failure model. The use of this failure model results in the CCF combinations and individual component failures of the same failure mode (e.g., FTR, FTS, etc.) being included in the CCF cutsets. For example, a CCF basic event for an NPP with three EDGs for the FTR failure mode will result in the following CCF cutsets in the overall CCF probability calculation:

– $\{A_i, CCF_{BC}\}$

– $\{B_i, CCF_{AC}\}$

– $\{C_i, CCF_{AB}\}$

– $\{CCF_{ABC}\}$

Because these CCF cutsets are included within a single CCF basic event and are limited to the same failure mode, not all CCF cross-products (e.g., CCF_{AB} FTR, C_i FTS) will be represented in the SPAR model cutsets. This modeling approach only affects the CCF modeling of CCCGs of three or more components. In addition, the missing CCF cross products will not have a significant risk impact in most ECAs. However, if missing CCF cross-products could have significant impact on ECA results, analysts should contact the SPAR Model Help Desk for assistance in modeling all the CCF cross-products.

5.8 General Treatment of Potential CCF in ECA

The adjustment of CCF probabilities given observed failures in ECAs allows the SPAR model to provide an approximate insight as to the risk significance of implicit environmental or organizational factors. CCF is the principal means (with HRA being the other) by which current PRAs (including the SPAR models) can assess the impact of organizational factors on risk, however approximate the assessment may be.

5.8.1 Key Principles

The key principles to evaluating potential CCF in ECAs provided in NUREG-2225 are summarized in the following subsections.[26]

[26] These key principles were derived with a specific focus on SDP evaluations. However, these principles apply to ECAs performed as part of other NRC Programs (e.g., ASP and MD 8.3). It is noted that the first principle was intended to avoid focusing an SDP evaluation on the specific manifestation of a failure at the piece-part level and note that a proximate cause could result in different piece part failures on redundant equipment. This issue is less a concern for ECAs performed as part of the ASP Program and MD 8.3 since these analyses do not define the causal level to be considered. Given the broader focus of ASP Program and MD 8.3 ECAs (i.e., these analyses do not generally focus on a proximate cause), the use of the alpha factor model to represent CCF potential is fully appropriate for these applications.

5.8.1.1 Potential for CCF is Treated at the PD (i.e., Proximate Cause) Level

ECAs performed as part of the SDP assess the PD at the level of the proximate cause of the degraded condition, not the degraded condition itself. Therefore, the organizational impact of the PD can propagate to other components within the CCCG through the existing coupling factors. As such, a PD can result in the failure of other components within the CCCG by any potential failure mechanism or by any piece-part failure related to the proximate cause. Another important effect of this key principle is that component failures within a defined CCCG caused by a PD are not treated as "independent" (i.e., having no potential for resulting in a CCF failure) in the SDP risk assessment. This is not to be confused with data collection activities that will make the determination of whether an observed failure is considered "independent" or is an actual CCF for the purposes of data coding and parameter estimation.

5.8.1.2 The Alpha Factor Method is Used by the NRC to Calculate All CCF Probabilities

The alpha factor method is a state of practice CCF method consistent with the ASME/ANS PRA Standard, is used by the NRC, and is one of the CCF methods used within the nuclear industry. The alpha factor method aligns with the current NRC data collection practices and allows for efficient estimation of base SPAR model CCF probabilities. In addition, the alpha factor method is designed to provide revised CCF probabilities that are adjusted when a component within a defined CCCG fails. The calculation of revised CCF probabilities using a reformulation of the basic parameter model, which SAPHIRE automatically performs using the SPAR models, follows the process shown in Appendix E of NUREG/CR-5485. While there is potential for these revised CCF probabilities to be either conservative or nonconservative, the alternative of maintaining the CCF probabilities at their base SPAR model values (i.e., not adjusted upon the observed failure) will always underestimate the risk significance of identified PDs.

5.8.1.3 Demonstration of the Functionality of Redundant Components within the Same CCCG Does not Eliminate or Reduce the Potential for CCF

Extent of condition evaluations or testing of redundant components is often mentioned to show that there is no CCF potential (beyond the base SPAR model CCF probability) given an observed failure. These extent-of-condition evaluations or testing measures are needed to verify the operability of redundant component(s) to establish compliance with TS. However, these measures cannot be used to show that potential CCF is reduced or eliminated in ECAs. In fact, CCF likelihood estimates for most typical components, even when adjusted upon the observed failure, would show a very low likelihood for the occurrence of an actual CCF event. Therefore, the normal expectation is that extent-of-condition testing would show that the redundant equipment was functional. However, if credit were provided for such extent of condition measures, ECAs would fail to account for the small, but potentially risk significant, chance that the PD or proximate cause could propagate to the redundant train(s). Therefore, such credit would be inconsistent with the established "failure memory approach", which assumes that a component with an observed success during an operational event still has a failure potential in a retrospective risk assessment.

5.8.1.4 Potential for CCF is limited to Redundant Components within the Same CCCG

Coupling factors between components within the same CCCG in the base SPAR model are presumed to exist because the CCCGs should be evaluated with the factors defined in the ASME/ANS PRA Standard. Even though some CCF coupling factors are not limited by CCCG boundaries, modeling of intersystem CCF is beyond the current state of practice in NPP PRAs. Therefore, potential CCF must be limited to redundant components within the same CCCG.

5.8.2 Deviations from Key Principles

Because a typical PRA does not model components to the piece part level, it is possible that some proximate causes cannot be shared among components that are redundant from the perspective of the PRA model. In other words, from a high-level perspective such as component type and function, components may be placed into the same CCCG in the PRA, but there may be differences at a lower level that are important to take into consideration. In these cases, the CCCG may have been defined in a simplified manner that does not account for these component differences. Conditioning CCF probability on the assumption of a common coupling factor in this case could produce an unnecessarily conservative estimate of risk. However, caution should be exercised in revising CCCG boundaries, because typical PDs which reflect organizational problems such as poor maintenance or corrective actions, can affect all the equipment within the CCCG despite the component differences. Because the proximate cause is defined at a higher level than the piece part failure mechanism, it is expected that situations requiring this deviation would be extremely rare.

A second category where the key principles may not strictly apply is also related to the level of detail in the PRA model. For example, a licensee's PRA may have explicit treatment of some dependencies that are treated implicitly via CCF in the associated SPAR models. Two examples are shared equipment that is not explicitly modeled in the PRA and latent (pre-initiator) human failure events (HFEs). For example, consider a power supply that is shared among all steam generator power-operated relief valves (PORVs), where this dependency is not explicitly included in the fault trees of the associated SPAR model. In this case, failure of the shared power supply (that would lead to multiple dependent PORV failures) could be captured by the PORV CCF basic event. However, to accurately model the impact of a PD that led to failure of the power supply, the analyst should modify the PRA model to capture this dependency explicitly. The other generic example related to the level of detail is pre-initiator or latent HFEs (e.g., miscalibrations). These are not treated comprehensively in some PRA models and again are captured indirectly by including such events in the alpha factor estimates. In this latter case, it is preferable to explicitly add the associated pre-initiator or latent HFEs to the PRA logic rather than relying on a qualitative argument.

A third category of potential deviations may arise for rare and exceptional circumstances where licensee defenses for CCF are not captured in historical operating experience and, therefore, not reflected in current CCF parameter estimates. This should not include routine state of practice CCF defenses have been implemented by licensees for many years and are reflected in current CCF parameter estimates. Examples of these routine CCF defenses include staggering of equipment modifications and testing, separation of redundant equipment to minimize environmental impacts, use of different maintenance staff, and standard quality assurance practices. For this deviation to apply, the risk analyst must determine that the CCF defense goes beyond the current state of practice, has not been widely implemented, and therefore is not already reflected in current CCF parameter estimates.

5.9 Different Cases for Treatment of Potential CCF in ECA

5.9.1 Failure of One Redundant Component

In ECAs where one of multiple, redundant components has failed, potential CCF needs to be considered. If the failed component is part of an existing CCCG in the SPAR model, the evaluation of potential CCF of the redundant components is straightforward. The analyst should set the appropriate basic event for the correct component and failure mode (e.g., FTS, FTR, FTO, FTC, etc.) to TRUE.[27] If the failed component is not part of an existing CCCG, a new one should be created in consultation with SPAR Model Help Desk. Once the new CCCG is added to the base SPAR model, the analyst can use the same process described above to properly account for potential CCF in the ECA. However, CCF parameters may not be available for the failed component type. In these cases, an analyst can use the generic demand or rate CCF parameters in the ECA. In addition, the analyst can contact the SPAR Model Help Desk for new CCF parameter templates.

5.9.1.1 Calculation Example

For a CCCG of three components (A, B, and C) with 1 out of 3 success criteria, there are the following four system cutsets:

- *{A_i, CCF_{BC}}*
- *{B_i, CCF_{AC}}*
- *{C_i, CCF_{AB}}*
- *{CCF_{ABC}}*

The system failure probability (per failure mode) using the basic parameter model can be represented as:

$$Q_S = {Q_1}^3 + 3Q_1Q_2 + Q_3$$

And the CCF portion of the system unavailability (i.e., the base CCF probability) is:

$$Q_{Base\_CCF} = 3Q_1Q_2 + Q_3$$

Where:

$$Q_1 = A_i = B_i = C_i$$

$$Q_2 = CCF_{AB} = CCF_{BC} = CCF_{AC}$$

$$Q_3 = CCF_{ABC}$$

The Q_k values can be calculated using the following equation:

$$Q_k^{(m)} = \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t$$

Where:

$$\binom{m-1}{k-1} = \frac{(m-1)!}{(k-1)!\,(m-k)!}$$

Which results in the following:

[27] The basic event should be set to TRUE in NRC ECAs to ensure the potential for CCF is properly estimated. The basic event probability should only be set to 1.0 a deviation of the key CCF principles is identified (see Section 5.8.2 for additional information).

$$Q_1^{(3)} = \frac{1}{\binom{m-1}{k-1}}\alpha_1 Q_t = \alpha_1 Q_t$$

$$Q_2^{(3)} = \frac{1}{\binom{m-1}{k-1}}\alpha_2 Q_t = \frac{1}{2}\alpha_2 Q_t$$

$$Q_3^{(3)} = \frac{1}{\binom{m-1}{k-1}}\alpha_3 Q_t = \alpha_3 Q_t$$

Given an observed failure of component 'A', A_i will be set to TRUE (i.e., probability set to 1.0) and the CCF basic events with component 'A' in them (CCF_{AB}, CCF_{AC}, and CCF_{ABC}) are conditioned on the observed failure. The other CCF basic event (CCF_{BC}) will remain at its nominal value (i.e., Q_2). Therefore, following the process provided in Appendix E of NUREG/CR-5485, the conditional CCF probability (Q_{CCF}) can be represented as:

$$Q_{Conditional\_CCF} = Q_2\left(\frac{Q_1}{Q_t}\right) + 2Q_1\left(\frac{Q_2}{Q_t}\right) + \frac{Q_3}{Q_t}$$

Where:

$$\frac{Q_1}{Q_t} = \alpha_1$$

$$\frac{Q_2}{Q_t} = \frac{1}{2}\alpha_2$$

$$\frac{Q_3}{Q_t} = \alpha_3$$

Therefore:

$$Q_{Conditional\_CCF} = Q_2\alpha_1 + Q_1\alpha_2 + \alpha_3$$

Assuming the CCCG is comprised of three EDGs for the FTR failure mode (Q_t = 2.678×10^{-2}), the mean alpha factors, provided in INL/EXT-21-62940, are:[28]

$$\alpha_1 = 0.986$$

$$\alpha_2 = 1.10 \times 10^{-2}$$

$$\alpha_3 = 3.48 \times 10^{-3}$$

[28] Note the alpha factors in this example sum to a value greater than 1.0 due to the use of the mean values from the individual alpha factor parameter distributions and rounding. By definition, the alpha factors for each specific component, failure mode, and CCCF size should sum to 1.0.

Therefore, the Q_k values are calculated as:

$$Q_1^{(3)} = (0.986)(2.678 \times 10^{-2}) = 2.64 \times 10^{-2}$$

$$Q_2^{(3)} = (0.5)(1.10 \times 10^{-2})(2.678 \times 10^{-2}) = 1.47 \times 10^{-4}$$

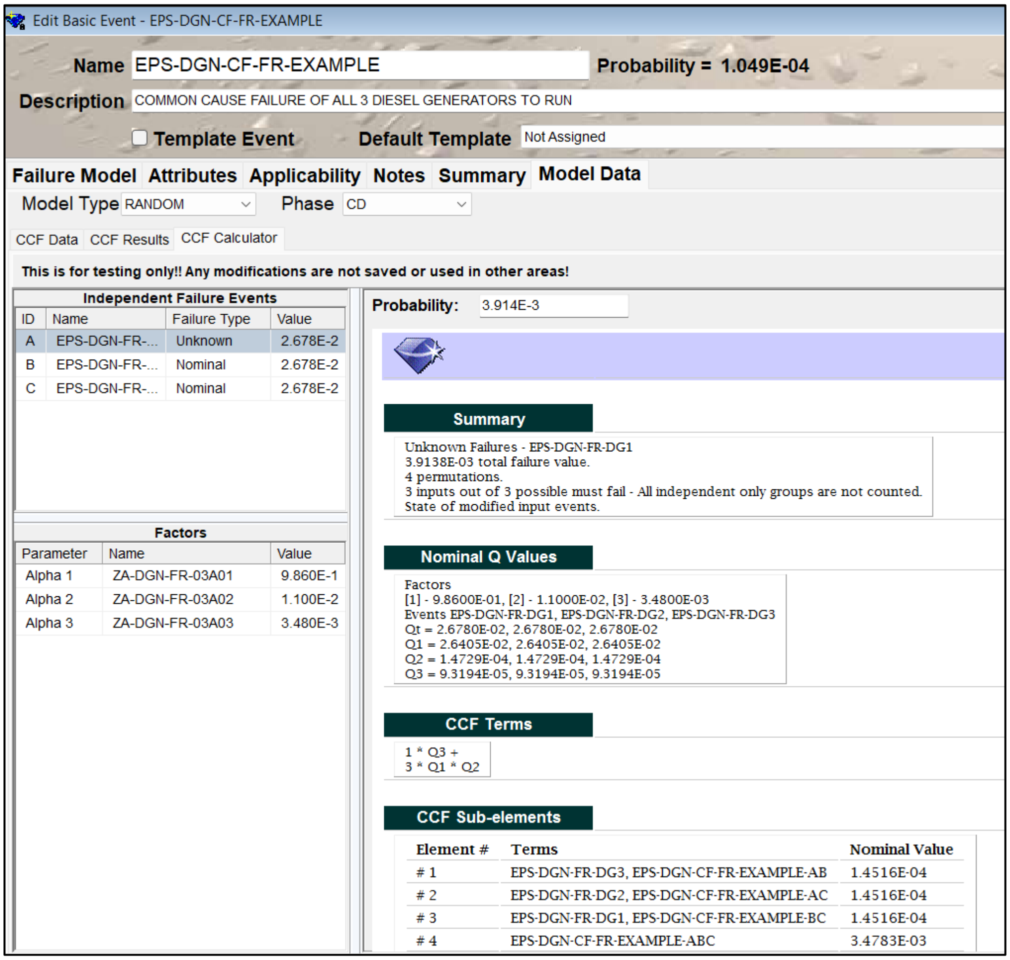
$$Q_3^{(3)} = (3.48 \times 10^{-3})(2.678 \times 10^{-2}) = 9.32 \times 10^{-5}$$

With the calculated Q_k values and the existing alpha factors, the base and conditional CCF probabilities are calculated as:

$$Q_{Base\_CCF} = (3)(2.64 \times 10^{-2})(1.47 \times 10^{-4}) + (9.32 \times 10^{-5}) = 1.049 \times 10^{-4}$$

$$\begin{aligned} Q_{Conditional\_CCF} &= (1.47 \times 10^{-4})(0.986) + (2.64 \times 10^{-2})(1.10 \times 10^{-2}) + (3.48 \times 10^{-3}) \\ &= 3.914 \times 10^{-3} \end{aligned}$$

SAPHIRE performs the conditional CCF probability calculation automatically when the applicable basic event associated with the observed failure is set to TRUE. Figure 5-1 provides a screenshot of the SAPHIRE CCF Calculator results for this example.



Name EPS-DGN-CF-FR-EXAMPLE Probability = 1.049E-04

Description COMMON CAUSE FAILURE OF ALL 3 DIESEL GENERATORS TO RUN

☐ Template Event Default Template Not Assigned

Model Type RANDOM Phase CD

This is for testing only!! Any modifications are not saved or used in other areas!

Independent Failure Events

ID	Name	Failure Type	Value
A	EPS-DGN-FR-...	Unknown	2.678E-2
B	EPS-DGN-FR-...	Nominal	2.678E-2
C	EPS-DGN-FR-...	Nominal	2.678E-2

Factors

Parameter	Name	Value
Alpha 1	ZA-DGN-FR-03A01	9.860E-1
Alpha 2	ZA-DGN-FR-03A02	1.100E-2
Alpha 3	ZA-DGN-FR-03A03	3.480E-3

Probability: 3.914E-3

Summary

Unknown Failures - EPS-DGN-FR-DG1
3.9138E-03 total failure value.
4 permutations.
3 inputs out of 3 possible must fail - All independent only groups are not counted.
State of modified input events.

Nominal Q Values

Factors
[1] - 9.8600E-01, [2] - 1.1000E-02, [3] - 3.4800E-03
Events EPS-DGN-FR-DG1, EPS-DGN-FR-DG2, EPS-DGN-FR-DG3
Qt = 2.6780E-02, 2.6780E-02, 2.6780E-02
Q1 = 2.6405E-02, 2.6405E-02, 2.6405E-02
Q2 = 1.4729E-04, 1.4729E-04, 1.4729E-04
Q3 = 9.3194E-05, 9.3194E-05, 9.3194E-05

CCF Terms

1 * Q3 +
3 * Q1 * Q2

CCF Sub-elements

Element #	Terms	Nominal Value
# 1	EPS-DGN-FR-DG3, EPS-DGN-CF-FR-EXAMPLE-AB	1.4516E-04
# 2	EPS-DGN-FR-DG2, EPS-DGN-CF-FR-EXAMPLE-AC	1.4516E-04
# 3	EPS-DGN-FR-DG1, EPS-DGN-CF-FR-EXAMPLE-BC	1.4516E-04
# 4	EPS-DGN-CF-FR-EXAMPLE-ABC	3.4783E-03

Figure 5-1. SAPHIRE CCF Calculator Result

5.9.2 Failure of Multiple Redundant Components in the Same CCCG due to the Same Cause

If two or more redundant components within the same CCCG fail due to the same cause, but a complete CCF has not occurred, a similar process described for the failure of one redundant component is used. The analyst should set the appropriate basic events (i.e., correct component and failure mode) to TRUE and SAPHIRE will automatically adjust the CCF probability.

5.9.3 Failure of Multiple Components in Different CCCGs

If two or more components fail, but are part of different CCCGs, the analyst will follow the same guidance as multiple components within the same CCCG fail. However, SAPHIRE will automatically adjust multiple CCF probabilities in this case. If the failures are the results of the same cause, analysts should consider the lack of intersystem CCF as a key modeling uncertainty, which should be evaluated quantitatively, if possible. For example, if multiple breakers associated with different systems fail due to the same cause, an increased breaker failure probability to account for the increased likelihood of intersystem CCF of similar breakers within the plant should be considered.

5.9.4 Failure of Multiple Redundant Components in the Same CCCG due to Different Causes (ASP only)

If two or multiple redundant components within the same CCCG fail due to different causes, certain CCF combinations within the CCCG cannot occur. Continuing the example of a CCCG of three EDGs, there are four potential CCF combinations:

– CCF_{AB}

– CCF_{BC}

– CCF_{AC}

– CCF_{ABC}

If EDG ‘A’ fails due to a design issue and EDG ‘C’ fails due to a maintenance issue, any CCF combination with both EDGs ‘A’ and ‘C’ (CCF_{AC} and CCF_{ABC}) are eliminated from further evaluation as part of the normal Boolean reduction process. This would result in CCF being limited to combinations CCF_{AB} and CCF_{BC}. To perform the CCF treatment required for this case, the analyst will need to contact the SPAR Model Help Desk to make the necessary modeling changes. These changes will result in the CCF combinations being expanded (instead of single CCF basic event), allowing them to manual adjusted in SAPHIRE. Once the required changes have been completed in the base SPAR model, the analyst will set the appropriate basic events (i.e., correct component and failure mode) associated with failures to TRUE. In addition, the basic events representing the CCF combinations that include the failed components should be set to FALSE (note that this has the potential of slightly underestimating the CCF potential since there still may be potential coupling factors between the failed components and the non-failed component). SAPHIRE will automatically calculate the adjusted CCF probabilities of the possible CCF combinations.

5.9.5 Failure of One Redundant Component Included in SSIE Fault Tree Modeling

As stated in Section 11.4, if a support system component fails, the analyst should set the applicable enabling basic event to TRUE and the component initiating event (if modeled) to FALSE. If the failed component is in a mitigating CCF basic event in an SSIE fault tree, the CCF probability will be recalculated using the normal process described in Section 5.8.1. The setting of the component initiating event to FALSE is potentially nonconservative; however, this approach is the current state of practice agreed upon between the NRC and Electric Power Research Institute.

5.9.6 One or More Redundant Components Are Degraded in the Same CCCG

If a degraded component is identified, the analyst should adjust the failure probability within the ECA. If the affected component is within an existing CCCG, SAPHIRE will automatically adjust the CCF probability. However, the adjustments made are limited by the existing CCF models.

Continuing the example of a CCCG of three EDGs, if EDG 'A' is degraded to where the FTR probability is increased to 0.1 (from its base probability of 2.678×10^{-2}), only the Q_1 value for EDG 'A' will be recalculated. The Q_2 and Q_3 values, which dominate the CCF probability, will remain unaffected because the Q_t used in the SAPHIRE CCF calculation remains at its base probability. As previously noted, the existing CCF models only allow a single Q_t for CCF probability calculations. Therefore, changes in CCF probabilities are expected to be small for cases where not all redundant components are degraded. If all the components within the CCCG are degraded, the corresponding Q_t will change, resulting in larger increases in CCF probability. For the above example of FTR probability being increased to 0.1, the CCF probability would increase from 1.05×10^{-4} to 1.16×10^{-4} for a single degraded EDG, 1.37×10^{-4} for two degraded EDGs, and 5.11×10^{-4} when all three EDGs are degraded.

5.9.7 Redundant Component(s) Unavailable due to Test/Maintenance

Components that are unavailable due to testing or maintenance during an event or applicable exposure time are modeled explicitly in ECAs performed as part of the ASP Program or MD 8.3. In ECAs where the applicable component(s) are part of an existing CCCG, the potential for CCF still exists. Specifically, redundant components could share a failure cause with the component unavailable due to maintenance, which would be "hidden" due to the maintenance unavailability. For these cases, the analyst needs to set the applicable component test/maintenance basic event(s) to TRUE, and SAPHIRE will automatically adjust the applicable CCF probability.

Continuing the example of a CCCG of three EDGs, if EDG 'A' is unavailable due to planned maintenance, the conditional CCF failure is represented by the following equation:

$$Q_{Conditional\_CCF} = 2Q_1Q_2 + Q_2 + Q_3$$

Using the same Q_k values calculated in Section 5.8.1.1, the conditional CCF probability is calculated as:

$$Q_{Conditional\_CCF} = (2)(2.64 \times 10^{-2})(1.47 \times 10^{-4}) + (1.47 \times 10^{-4}) + (9.32 \times 10^{-5}) = 2.48 \times 10^{-4}$$

6 Modeling Recovery and Repair

6.1 Objective and Scope

This section provides guidance for the treatment of recovery and repair actions of a failed or degraded SSC. The guidance addresses what recovery and repair actions should be credited in ECAs, and the requirements that should be met before crediting such actions. Definitions for recovery and repair action are provided. Also, guidance and considerations are provided for conducting recovery analyses and for modeling recovery/repair actions in the SPAR model. This section applies to ECAs in SDP, ASP, NOED or MD 8.3 assessments.

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

6.2 Background

In PRA, there is a clear distinction between actions to repair components or systems and actions to recover components or systems. The following definitions are from NUREG/CR-6823 and the ASME/ANS PRA Standard.

6.2.1 Recovery Actions

Recovery actions involve the use of alternate equipment or means to perform a function when primary equipment fails, or the use of alternate means to utilize equipment that has not responded as required. The ASME/ANS PRA Standard defines recovery actions as "*. . . restoration of a function lost as a result of a failed SSC by overcoming or compensating for its failure.*"

> Examples of recovery actions include opening doors to promote room cooling when a heating, ventilation, and air conditioning system fails, recovering grid-related losses of offsite power by rerouting power, manually initiating a system when the automatic actuation signal fails, bypassing trip logic using jumper cables, and using a hand wheel to manually open a motor-operated valve when the motor fails to operate.

6.2.2 Repair Actions

Repair actions involve the actual repair of the mechanism, which caused a component or system to fail. The ASME/ANS PRA Standard defines repair as *". . . restoration of a failed SSC by correcting the cause of failure and returning the failed SSC to its modeled functionality.*"

> Examples of repair actions include repairing weather-related LOOPs, repair of a pump that failed to start, or replacement of a failed circuit breaker.

6.2.3 Overview: Modeling Recovery and Repair Actions in PRAs

Recovery can involve complicated actions that are governed by procedures and are typically evaluated using HRA methods. A general exception is the treatment of offsite power recovery where the required recovery actions are often not within the control of the plant personnel. Thus, offsite power recovery data is collected and evaluated for use in PRAs. Recovery of an EDG is another action commonly modeled in PRAs based on actual data. The repair of other components is generally not modeled in base PRA models because one or more of the following apply to most cutsets and sequences: (1) the time available to repair most components is generally too limited (i.e., core damage would occur before the repair is completed), (2) repair is an action that is not governed by abnormal operating procedures (AOPs)/EOPs and thus difficult to justify, (3) the availability of spare parts can challenge performance, and (4) AOPs generally direct operators to use alternative equipment as a first priority.

HRA techniques for estimating the likelihood of successful repair should not be used because the possible repair scenarios are affected by a variety of human actions and hardware-related issues that would not be known without understanding the specific causes of the problem.

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

6.3 Treatment of Recovery/Repair Actions in ECA – General[29]

6.3.1 ASME/ANS PRA Standard Requirements

Actions to recover/repair an observed failure of an SSC can be considered and modeled in accordance with supporting requirements of the ASME/ANS PRA Standard. For the most part, the applicable supporting requirements can be used to model recovery and repair actions in an event assessment. An overview of applicable high-level and supporting requirements includes the following considerations:

- Demonstration that the action is plausible and feasible for the scenarios to which recovery/repair action is applied (HLR-HR-H).
- Availability of procedures, operator training, cues, and manpower (HR-H2).
- Relevant scenario-specific performance shaping factors (PSFs)/performance influencing factors (PIFs) in the HRA (HR-H2 and HR-G3).
- Dependencies between HFEs (recovery, repair, and EOP actions) in the sequence, scenario, or cutset (HR-H3, HR-G7, and QU-C2).

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

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

6.3.2 Using Data to Estimate Non-Recovery Probabilities

The nominal failure probability for a repair action is normally based on the evaluation of industry-wide operating experience data. Examples of data-based non-recovery probabilities used in SPAR models include recovery/repair of EDG failures and LOOP events. Guidance on the process for collecting and evaluating recovery and repair data is provided in Section 5.3 of NUREG/CR-6823. This guidance includes a description of the type of data that is reviewed and guidelines for allocating data. Analysts specializing in parameter data collection, reduction, and statistical analysis should be consulted for estimating a non-recovery probability using operational experience data.

6.3.3 Using HRA to Estimate Non-Recovery Probabilities

Failure probability for a recovery action is normally derived in an HRA. Good practices from NUREG-1792, "Good Practices for Implementing Human Reliability Analysis," (ML051160213) for crediting post-initiator recovery actions while implementing RG 1.200 and the related requirements of the ASME/ANS PRA Standard are summarized below.

6.3.3.1 Good Practice #1: Define Appropriate Recovery Actions

Based on the failed functions, systems, or components, identify recovery actions to be credited that are not already included in the PRA (e.g., aligning another backup system not already accounted for) and that are directed to be implemented by the crew to restore the failure. Aspects to consider are included in the questions listed in Section 6.6.

6.3.3.2 Good Practice #2: Account for Dependencies

The good practices provided for post-initiator HFEs in general apply specifically to recovery actions as well.[30] Particular attention should be paid to accounting for dependencies among the HFEs including the credited recovery actions. Considerations for accounting for dependencies are provided in Section 6.4 and Section 6.7.

6.3.3.3 Good Practice #3: Quantify the Probability of Failing to Perform the Recovery

Quantify the probability of failing to perform the recovery by (1) using representative data that exists and deemed appropriate for the recovery event, or (2) using the HRA method/tool(s) used for the other HFEs (i.e., using an analytical/modeling approach). If using data, ensure the data are applicable for the plant/sequence context or that the data are modified accordingly.

In addressing the above issues and assessing which recovery action, or actions, to credit in the PRA, for post-initiator HFEs all the good practices provided in the following sections in NUREG-1792 apply (i.e., the failure to recover is merely another HFE, like all of the other post-initiator HFEs):

- Section 5.1, "Identifying Potential Post-Initiator HFEs"
- Section 5.2, "Modeling Specific HFEs Corresponding to Human Actions"
- Section 5.3, "Quantifying the Corresponding Human Error Probabilities (HEPs) for Post-Initiator HFEs"

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

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

6.4.1 Considerations for Determining Recovery/Repair Actions are Plausible and Feasible

A thorough recovery analysis requires careful consideration (at the cutset or scenario level) of the appropriate PSFs/PIFs in the HRA. Some questions to consider for crediting and modeling the recovery/repair of an observed failure are provided in Section 6.6. These questions were developed largely from the ASME/ANS PRA Standard, NUREG-1792, and experience from SDP and ASP analyses.

6.4.2 Exceptions to Requirements and Considerations

In general, no recovery or repair action should be credited where any of the considerations in Section 6.7 are not met (e.g., there is not sufficient time, there are no cues that there is a problem, there are not sufficient resources, and there is no procedure or training). It may be possible to justify exceptions in unique situations, such as a procedure is not needed because the recovery/repair is a skill-of-the-craft, non-complex, and easily performed; or the specific failure mode of the equipment is known for the sequence (this is usually not the case at the typical level of detail in a PRA) and so repair of the failure can be credited because it can be easily and quickly diagnosed and implemented. Any exceptions should be documented as to the appropriateness of the recovery/repair action.

6.4.3 Consideration of Observed Errors, Failures, and Successes

Once an observed failure was judged recoverable or repairable given cutset-specific time constraints, the failure probability for a recovery or repair action can be estimated based on cutset-specific HRA and observations from the actual repair of the component. Difficulties, errors, and failures that were observed during the recovery/repair should be considered in the HRA (and in the recovery/repair plausibility and feasibility determination). This is consistent with the "Failure Memory Approach."[31] Similarly, recovery/repair actions that were performed successfully during the event should be addressed in cutset-specific HRAs, given that successes are treated probabilistically in the "Failure Memory Approach."

6.4.4 Consideration of Operator Intervention Preventing a Catastrophic Failure

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

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

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

leak.

6.4.5 Consideration of Support System Availabilities

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

6.4.6 Examples of Failure Events and Associated Potential Recovery Actions

Table 6-1 below provides examples of failure events and associated potential recovery actions.

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

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

6.4.7 Modeling Recovery of Test and Maintenance Unavailabilities

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

6.4.8 Modeling Multiple Recovery/Repair Actions

Considerations for crediting and modeling more than one recovery/repair actions (i.e., how many recoveries to be credited in one accident sequence/cutset) include the following:

– Recovery/repair of failures in one system should be limited to one failed component in the system (i.e., recovery/repair limited to one train in a multiple train system).

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

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

  For example, diagnosing and recovering simultaneous failures of the AFW and high-pressure injection systems may be difficult within the short time available, whereas recovery of AFW (required early in most sequences) and RHR systems (required for late, long-term cooling) may be more likely. A quick recovery of one system involving trip reset from the control room may allow operators to diagnose and recover another system failure.

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

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

6.4.9 Consideration of Alternate Mitigating Strategies

Plant licensees have implemented alternate mitigating strategies (e.g., B.5.b. measures, FLEX) in response to NRC orders. These strategies often involve the use of non-safety, portable, manually controlled, offsite, or non-standard system alignments. Crediting of these strategies in ECAs should meet the guidelines outlined in Regulatory Information Summary 2008-15, “NRC Staff Position on Crediting Mitigating Strategies Implemented in Response to Security Orders in Risk-Informed Licensing Actions and in the Significance Determination Process,” (ML080630025). Consideration for incorporation of manual actions, special equipment operation, or other non-standard actions into ECAs include, but are not limited to:

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

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

Nuclear Energy Institute's (NEI) FLEX in Risk-Informed Decision-Making (FRIDM) Task Force developed guidelines for the industry to follow when requesting credit for alternate mitigating strategies. This guidance is contained in two white papers, "Qualitative Assessment for Crediting Portable Equipment in Risk-Informed Decision Making," (ML16138A018) and "Streamlined Approach for Crediting Portable Equipment in Risk-Informed Decision Making," (ML16138A017) The NRC has not endorsed this guidance; however, a letter from the NRR Office Director was issued (ML16167A034), which captured NRC staff's views on the white papers. NEI subsequently submitted NEI 16-06, "Crediting Mitigating Strategies in Risk-Informed Decision Making," (ML16286A297), for information only to the NRC. This document has three sections, the first two representing the contents of the two white papers and a third section providing guidance to licensees about crediting portable equipment in a PRA. This section was reviewed by NRR staff and a publicly available memorandum (ML17031A269) was issued in 2017 to capture the staff's comments. The staff updated its assessment of industry guidance for crediting mitigating strategies in PRAs in a publicly available memorandum (ML22014A084) in 2022. The above referenced documents should be considered information only to NRC risk analysts as background information on how licensees may credit alternate mitigating strategies in the ECAs.

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

6.4.10 Consideration of Dependencies among Multiple Human Actions in a Cutset

Particular attention should be paid to accounting for dependencies among HFEs, including the credited recovery/repair actions. Considerations from NUREG-1792 include:

- Dependence should be assessed:
  - Among multiple recoveries in the accident sequence/cutset being evaluated
  - Between each recovery and the other HFEs in the sequence/cutset being evaluated
- As part of this effort, the analyst should give proper consideration to the difficulties people often have in overcoming an initial mindset, despite new evidence.

  For example, consider how long the PORV path remained open in the Three Mile Island accident, despite new cues of the problem, different personnel arriving, etc.
- The determination of whether there is dependence between HFEs and the level of dependence (if there is dependence) needs to be adequately justified and documented to ensure that credit for the recovery action(s) is appropriate. Refer to Section 9.5 for further information on dependence.

6.4.11 Extending Recovery/Repair Time (FTR Events)

A component failure, after the component had operated for some of its mission time (even 10 minutes or so), can help to extend the time to core uncovery. Reduced decay heat rate, full steam generators (for PWRs), or a full reactor vessel (for BWRs) extends the time before core uncovery, thus allowing for more recovery/repair time.

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

The following sections provide some considerations when crediting recovery/repair from a FTR event.

6.4.11.1 Increase in Time Available for Diagnosis and Operator Actions

Extended time may increase the Time Available of the recovery/repair actions.

> For example, failure of the last running AFW pump at 3 hours after reactor trip would increase the available time to initiate feed and bleed actions due to lower decay heat rate and full steam generator(s).

6.4.11.2 Thermal-Hydraulic Basis of Event Tree Function

The basis for changing the success criteria of a system based on extended time to core damage from a FTR event should be compatible with the appropriate thermal-hydraulic response. The timing of sequences (core damage/uncovery times) used in event trees are usually based on the assumption that FTS and FTR events occur at t = 0.

6.4.11.3 Reduced Mission Time

Recovery/repair of a component that FTR will reduce the mission time that the component/system must run, after recovery/repair, to complete its 24-hour mission. However, the successful operation of the component/system before the failure must be probabilistically modeled (consistent with the “Failure Memory Approach”) in the PRA using nominal FTR probability during the first part of the mission time segment.

6.5 SPAR Model Modifications– Considerations

6.5.1 Consult the SPAR Model Help Desk

Changes to the SPAR model should be closely coordinated with the SPAR Model Help Desk staff to ensure changes are completely reflected throughout the model and changes are made in accordance with the SPAR model quality assurance program. Review checklists for SPAR model modifications are provided in Volume 3 of this handbook.

6.5.2 Where to Add the Recovery Event: Event Tree, Fault Tree, Sequence, or Cutset

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

The following sections provide considerations for adding a recovery event at the various levels in the SPAR model.[32]

6.5.2.1 Event Tree Level

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

6.5.2.2 Fault Tree Level

Modeling recovery and repair actions are nominally included at the fault tree level. However, as with event tree applications, post-processing rules may be needed to apply a time-dependent recovery action at the sequence or cutset level. Further, a modified fault tree with configuration-specific structure and/or probabilities may be required for unique event-specific situations. In this case, the analyst may find it easier to copy and rename an existing fault tree, modify as desired, and apply the new fault tree in a sequence via a linking rule.[33]

6.5.2.3 Sequence Level

Direct fault tree substation within the applicable event trees (s) or the creating new event tree linkage rules can be used to include the recovery and repair actions in the appropriate accident sequences within the SPAR model. Refer to the above for additional considerations for applying recovery/repair actions to fault trees.

6.5.2.4 Cutset Level

Applying recovery/repair actions at the cutset level is a common method for ensuring that the time-dependent nature of the recovery or repair action is properly modeled. Post-processing rules are used to replace or append an existing basic event in a cutset with another that includes the failure probability of the action. However, the applicable cutsets must be identified before the post-processing rules can be written. Considerations include:

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

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

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

6.5.3 Where to Apply the Recovery Event: Base Case Model or Non-Conforming Case

The analyst must decide whether to add the recovery or repair action in the base case SPAR model or the non-conforming case (or both). Applying a recovery/repair basic event in the base case model may lower baseline CDF, thus increasing the change in core damage frequency (ΔCDF) in select sequences. Applying the event in the non-conforming case and setting the event to FALSE in the base case model may increase baseline CDF, thus decreasing ΔCDF in select sequences. For most cases in ECA, applying a recovery or repair action to both cutsets associated with the observed failure will not result in a significant difference in the results. The following sections provide some considerations for modeling recovery and repair actions.

6.5.3.1 Applying Recovery Actions for Pre-Planned Strategies

Recovery actions for pre-planned strategies should be modeled in the base case SPAR model. These actions are usually pre-planned using installed systems with pre-staged hardware, tools, procedures, and training.

For a data-derived non-recovery probability already included in the base case model, the basic event parameter inputs (i.e., random failure data, uncertainty data) in the base case model may be replaced with the parameters associated with the HRA-derived estimate.

For an HRA-derived non-recovery probability already included in the base case model, human errors that were observed during the recovery/repair should be considered in a failure-specific HRA to re-evaluate the non-recovery probability. The basic event parameter inputs in the non-conforming case should include parameters associated with the HRA-derived estimate.

6.5.3.2 Applying Repair Actions for Observed Failures

Repair actions of observed failures can be modeled in the non-conforming case. The HEP will be failure specific. Event-specific risk reduction is usually credited in the non-conforming case. If a data-derived non-recovery probability is already included in the base case model (e.g., EDG repair), that value should remain in the base model with the HEP used in the non-conforming case.

6.5.4 Using an Existing Recovery Event in the SPAR Model

The base case SPAR model contains few recovery events that include basic events and post-processing rules with nominal failure to recover probabilities (e.g., EDG, LOOP). In addition, some SPAR models may include legacy events and rules that are not used (set to TRUE). Considerations for the use of an existing recovery event are summarized below and discussed further in the subsection. Recovery/repair actions in SPAR models are noted by “XHE-XL” in the basic event name.

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

Check that a proposed modification to an existing basic event or fault tree does not adversely impact the use of the same basic event or fault tree elsewhere in the SPAR model. The modification may not be appropriate in all sequences, especially for time-dependent recovery/repair actions. Some considerations include the following:

- Examples where a modification of a basic event can affect multiple parts of the model include:
    - ○ Basic events used in different fault trees,

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

6.5.4.2 Review SPAR Model Post-Processing Rules

Post-processing rules are free-form logic rules that allow for the alteration or deletion of fault tree or sequence cutsets in a “post-processing” fashion. Postprocessing rules are used in SPAR models to apply recovery/repair events and other types of basic events in the appropriate cutsets after the change set is generated and the sequences are solved.

The post-processing rules employed during the model solution should be reviewed to understand how the rules impact dominant cutsets. Such rules may remove cutsets or significantly reduce the cutsets’ probability. Confirm that any such rules are appropriate for the analysis and modify as necessary.

Postprocessing rules may be developed for the following cases:

- – Particular fault tree (Fault Tree Rule Level)
- – All fault trees (Project Rule Level)
- – Particular sequence (Sequence Rule Level)
- – Single event tree (Event Tree Rule Level)
- – All sequences (Project Rule Level)
- – A list of each type of recovery rule can be viewed in SAPHIRE.

6.5.5 Adding a Recovery Event in a Fault Tree

The following sections provide considerations for adding a new recovery event in an existing fault tree.

6.5.5.1 Include Nominal Failure Probabilities Associated with Restart

When modeling the recovery/repair of an observed failure, include nominal probability of hardware failures during and after restart attempt. Components can FTS and FTR after they are successfully recovered or repaired. This is important for failure modes with high failure probabilities (e.g., a failure mode probability that is on the same or greater than the non-recovery probability). Since the component event is set to TRUE, a sub-tree will be needed to model the recovery and operation of the component during restart and throughout the remainder of its mission time.

6.5.5.2 Example of Using the Correct Fault Tree Logic

An example of sub-tree logic for a repair model that can be added to an existing fault tree is shown in Figure 6-1.

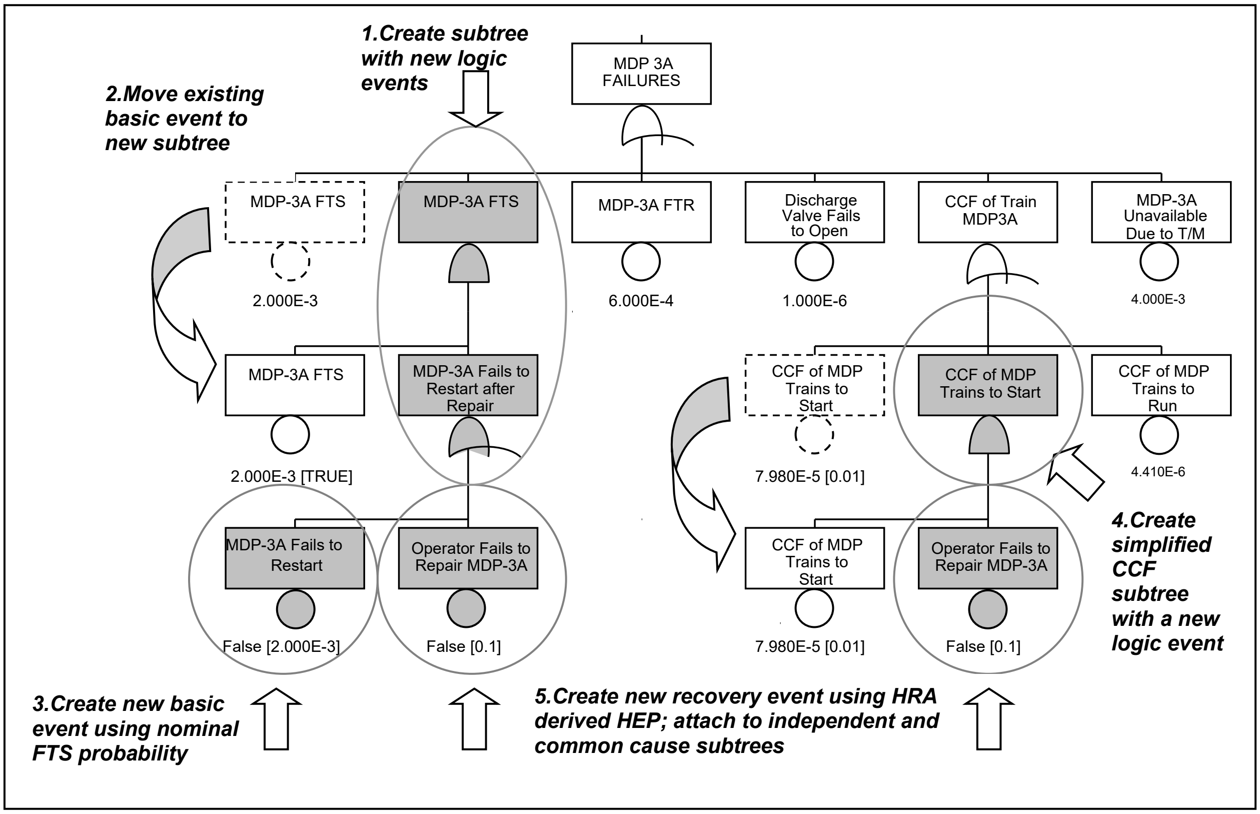

1.Create subtree with new logic events
2.Move existing basic event to new subtree
MDP 3A FAILURES
MDP-3A FTS
MDP-3A FTS
MDP-3A FTR
Discharge Valve Fails to Open
CCF of Train MDP3A
MDP-3A Unavailable Due to T/M
2.000E-3
6.000E-4
1.000E-6
4.000E-3
MDP-3A FTS
MDP-3A Fails to Restart after Repair
CCF of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

Figure 6-1. An Example of Sub-Tree Logic for a Repair Model Added to an Existing Fault Tree (The basic events in the figure show example base case and change set values).

Elements of the sub-tree example are summarized below.

- A new recovery event (*Operator Fails to Repair MDP 3A*) is created and the failure probability is set to the HRA-derived estimate (HEP = 0.1) in the non-conforming case to represent observed failure and cutset dependencies. If HEPs are cutset dependent, then post-processing rules are used to replace the “place holder” recovery event with the cutset-specific recovery events (not shown). Each of these recovery events will have a unique name and parameter values. This recovery event should be set to FALSE in the base case model.
- The original FTS basic event (*MDP-3A FTS*) is moved to the sub-tree, and the failure probability is set to TRUE in the non-conforming case. This basic event must remain in the model, since it is used in the CCF compound event for that failure mode (not shown). Note that the logic does not allow the propagation of the TRUE value up the tree.
- A new basic event (*MDP-3A Fails to Restart*) is created to model the probability of failure to restart following repair. This failure probability (and other basic event parameter inputs) is normally set to the nominal value for that failure mode, i.e., same parameters

used in the base case model basic event (*MDP-3A FTS*). This recovery event should be set to FALSE in the base case model.

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

6.5.5.3 Other Details

Some other details to consider in the above example are:

- The new basic event (*MDP-3A Fails to Restart*) probability can be updated to include recent operating experience as well as the observed failure as one more additional failure. The parameter update would be most important for rare or infrequent failure events. Refer to NUREG/CR-6823 for guidance in parameter estimations.
- For cases involving repair of a FTR event, the modification of the fault tree would be much the same as in the FTS example (replace the FTS-related events to FTR). The exception is that the FTR basic event parameter for mission time should be reduced to reflect the run time required to complete the remaining sequence mission time (usually 24 hours).

6.5.5.4 Consideration of Success Terms

When modifying a fault tree that results in a high failure probability (i.e., 0.1 to 1.0), consult the SPAR Model Help Desk for guidance on incorporating success terms in the model results. This is especially important for top events with a single basic event for the fault tree.

6.5.5.5 Update the Base Case SPAR Model

When adding a recovery event to a fault tree, make sure that the base case model is updated, as well as the non-conforming case model. Otherwise, a negative cutset importance may be calculated due to a lower core damage probability (CDP) or CDF of the base case SPAR model. For recovery actions, the recovery event in the base case model should be set to the failure-specific HEP. No changes should be made to the recovery event in the non-conforming case.

6.6 Questions to Consider for Crediting Recovery/Repair Action

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

- How long did the recovery/repair actually take?
- Was there any time pressure for the actual recovery/repair action?
- Were there any difficulties observed during the recovery/repair activity?
- What is the basis for assuming an earlier recovery/repair time than what was actually observed?

- When did the plant staff first determine that the recovery/repair action is plausible and feasible (but decided to defer an immediate action due to operability or availability of a redundant SSC)?
- Did a procedure for recovery/repair exist at the time of the event?
- Could the observed failure mechanism result (probabilistically) in a worse case failure that could not be recovered/repaired?

6.7 Considerations for Defining Appropriate Recovery/Repair Actions

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

- Can the failure be recovered/repaired given postulated extreme environmental conditions? Considerations include:
  - High temperatures due to high-energy line break,
  - Flooding from line breaks (e.g., floor drains overfill, overflow down stairways),
  - High radiation levels from containment sump recirculation,
  - Component accessibility,
  - Chemical hazard (e.g., transformer oil), and
  - Extreme weather (ice, high winds, lightning).
- What are the cues (e.g., alarms) that alert the operator to the need for a recovery action(s) and the failure that needs to be recovered? Will the cues be clear and provided in time for postulated sequences of interest?
- Is there sufficient time for the recovery action(s) to be diagnosed and implemented (repair failure, re-start system, and recover core cooling) to avoid the undesired outcome for postulated sequences? Time-dependent considerations include:
  - Time to core uncovery,
  - Time to recover vessel water level before pressure exceeds pump injection limits (low pressure (pump run-out), high pressure (pump shutoff head)),
  - Time to suppression pool over-pressure failure (BWR only), and
  - Time to suppression pool temperature exceeding net positive suction head limits (BWR only).
- Can the recovery/repair action be accomplished within the required time frame? Considerations include:
  - Tools readily available,
  - Spare parts readily available,
  - Area lighting and power sources for tools available,
  - Communications with control room available, and

  - Plant staffing level with the right skills.[34]

- Would the crew know how much time is available before core uncovery or other time sensitive considerations?
- Is the crew trained in the recovery action(s) and is the quality and frequency of the training adequate?
- Is there procedural guidance to perform the recovery?
- Is the equipment needed to perform the recovery available in the context of other failures and the initiator for the sequence/cutset? Are the support systems available in sequences in which recovery is credited?

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

7 Multi-Unit Considerations

7.1 Introduction

At a multiple unit site, an event or condition at one plant unit may affect other units. From the standpoint of MD 8.3 event assessments, the total risk impact on all units should be evaluated. If subsequent inspection of the event or condition identified a PD that impacts more than one unit, then a PD should be written for each affected unit, and an SDP assessment should be performed for each plant unit.

Frequently, multiple units at a given site are connected to benefit from pooling their system resources. In general, this turns out to be better than having half the 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, if the crosstie 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 that the two units compete for service water resources. If there are sufficient "system resources" and design margin, 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 CCCGs, 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 total redundancy of shared systems need careful attention, because they are not always risk-significant, but the potential exists.

7.1.1 Typical Shared Systems

Some systems that are shared to varying extent at sites include:

- Emergency alternating-current (AC) electrical power
  - EDGs
  - SBO diesel generators
  - AC power sources including hydroelectric generators and gas turbine generators
- DC electrical power
- Instrument air and station air,
- Raw water systems (e.g., service water, emergency service water (ESW), emergency equipment cooling water)
- Component cooling water
- AFW
- Condensate storage tank

- Chemical and volume control

7.1.2 Typical Site-Wide Initiators

Examples of event initiators that may impact multiple units include:

- LOOP
- Loss of service water
- Loss of instrument air
- Loss of a single AC or DC bus
- External events including seismic, high wind, and flooding.

7.2 Modeling Considerations

7.2.1 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.

7.2.2 Treatment of Shared Assets between Units

If a shared asset only has the capacity to support one unit at a time, then a “shared availability factor” logic event or sub-tree should be incorporated into the system fault tree that reflects the probability that the other unit will not need the asset to meet minimal functional success criteria. The shared availability factor should include the frequency of an appropriate dual unit initiator, HEPs of implementation actions, and hardware failure probabilities of appropriate failure modes.

7.2.3 Treatment of Operational Events Affecting Multiple Units at a Site

An operational event that impacts more than one plant at a multiple unit site should be evaluated for each unit separately. The risk analysis results for each unit should not be added together or integrated into one result.

7.2.4 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 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 the analysis. Furthermore, crediting the actual availability of the opposite unit’s AFW pump(s), versus nominal T/M values, would depend on the type of ECA being performed (e.g., SDP vs. ASP).

7.2.5 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 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 crosstied from the unaffected unit, can be credited at the affected unit.

- FTS, FTR, unavailability for T/M (including when the unaffected plant is in shutdown), and any operator action such as manual crosstie from the unaffected unit should be modeled appropriately.

7.2.6 Site-Wide LOOP Event

For a LOOP initiator affecting the site, modeling considerations include the following:

- The impact of the event or degraded condition(s) on all units should be assessed (e.g., swing EDG).
- Two plant units should not take full credit for the swing equipment at the same time.
- Carefully review TS and procedures for allowed and disallowed sharing or crosstie configurations.
- Review procedures to identify if one unit is given clear priority over another (e.g., a specific unit has priority for the SBO diesel generator).
- Shared support system dependencies such as ESW that can be crosstied to other unit(s) to support EDG cooling 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 actions. Recovery actions are less probable in a multi-unit LOOP than single-unit LOOP.
- Carefully review CCCGs and probabilities.
- Review cutsets carefully for logical consistency, specifically that all dominant cutsets are included and no illogical cutsets are indicated.

7.2.7 Other Initiators Affecting More than One Unit

For other initiators potentially affecting more than one unit, proceed in a similar manner to the LOOP case above:

- Consider the need to adjust the initiating event frequency based on operating experience to reflect impact on two or more units.
- Review relevant system fault trees where operator action to crosstie units is credited. Ensure the reasonableness of actual plant and operator response to an event (e.g., time available for operator response vs. feasibility of recovery actions under changing environmental conditions).
- Consider the need to modify applicable PSFs/PIFs in accordance with the HRA methodology.

7.3 Example of a Multi-Unit SDP Assessment

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

7.3.1 Unit 1 SDP Assessment

In Unit 1, a PD was identified which caused a degraded condition by which a random initiating event with subsequent reactor trip would result in a consequential LOOP. A month after the PD for the degraded condition was introduced in a transformer relay; Unit 1 was at power when it experienced a random reactor trip. The degraded condition resulted in a consequential LOOP that manifested itself through the random reactor trip. Since the PD did not cause the initiating event, the SDP assessment should calculate the change in core damage probability (ΔCDP) in a conditional analysis.[35]

7.3.2 Unit 2 SDP Assessment

Unit 2 was shut down and on shutdown cooling. In addition, electrical power to the operating RHR train in Unit 2 was being supplied from Unit 1 via an electrical crosstie. With the crosstie, the LOOP event in Unit 1 resulted in a subsequent loss of RHR in Unit 2. The same PD (inadequate maintenance control) impacted Unit 2 in two different ways: (1) the LOOP in Unit 1 resulted in the loss of RHR in Unit 2 and (2) an additional degraded condition (identical to that on Unit 1) was discovered in Unit 2.

7.3.2.1 Loss of RHR Event in Unit 2

At the time of the LOOP in Unit 1, Unit 2 was in cold shutdown and running on one RHR pump. The RHR pump was powered from an electrical crosstie from Unit 1. Therefore, the plant boundary for Unit 2 includes the crosstie up to and including the degraded condition in Unit 1 transformer relay. The PD that caused the LOOP in Unit 1 resulted in the loss of RHR in Unit 2. Given that the Unit 1 LOOP and subsequent loss of RHR manifested itself through the Unit 1 random reactor trip, the SDP should calculate the ΔCDP in a conditional analysis.[36]

7.3.2.2 Degraded Condition in Unit 2

The same PD was also introduced in Unit 2, which resulted in an additional degraded condition on an identical component and system (transformer relay) in Unit 2. Like Unit 1, the degraded condition in Unit 2 would result in a concurrent LOOP given a random reactor trip of Unit 2 (during at-power operations). Given that no random reactor trip was involved in Unit 2, the SDP should calculate the ΔCDP in a conditional analysis.[37]

7.3.2.3 Number of Findings in Unit 2

The PD impacted Unit 2 at two different time periods: (1) the degraded condition over the one-month exposure time prior to shutdown and (2) the loss of RHR initiating event during shutdown. Since the same PD impacted Unit 2 at two different time periods that were not overlapping, the risk impacts are additive. Thus, one finding for Unit 2 is appropriate because the PD is the same.[38]

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

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

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

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

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

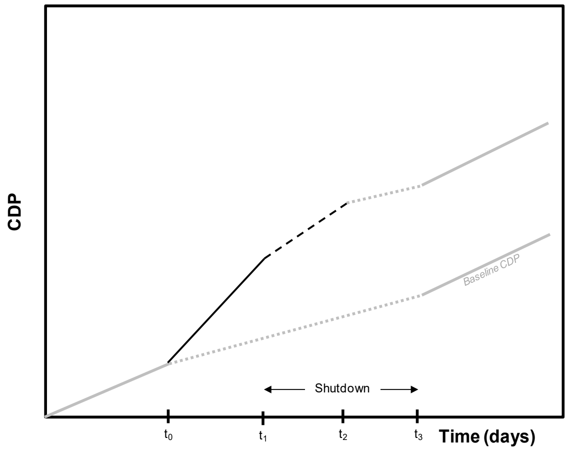


Figure 7-1a. CDP vs. Time for Example (Unit 2)

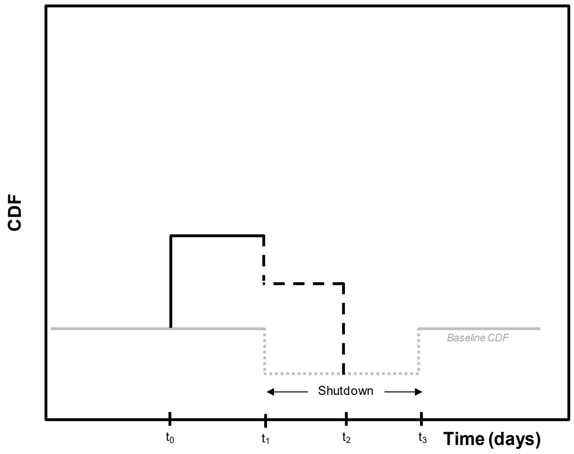


Figure 7-1b. CDF vs. Time for Example (Unit 2)

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

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

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

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

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

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

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

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

8 Initiating Events Analyses

8.1 Objective and Scope

This section provides guidance on the treatment of initiating events during at-power operation in ECAs. This section discusses the treatment of initiating events with and without a concurrent degraded condition. For SDP evaluations, a PD must have caused the observed initiating event. If the same PD also resulted in a degraded condition, the SDP evaluation will also need to consider its risk impacts. The identification of a PD is not required for ASP or MD 8.3 assessments.

Treatment cases that are in the scope of this guide are summarized below.[39]

- *Case 1– Initiating event only.* An initiating event with subsequent reactor trip occurs. No concurrent degraded conditions were experienced during the event.
- *Case 2– Initiating event and concurrent degraded condition(s).* An initiating event with subsequent reactor trip occurs. In addition, concurrent degraded condition(s) must have occurred for this case. For SDP evaluations, the same PD must be the cause of the initiating event and the concurrent degraded condition(s).
- *Case 3– Initiating event and mutually exclusive degraded condition(s) (SDP only).* The same PD causes an initiating event with subsequent reactor trip and mutually exclusive degraded condition(s).[40]

For all three cases, the treatment of test/maintenance should be made according to the applicable program-specific guidance. Note that this section does not address recovery of functions lost because of the initiating event such as loss of MFW, condenser heat sink, etc. Refer to the Section 6 on modeling recovery for additional information.

The following cases are outside the scope of this guide:

- Failure of support system component(s) that did not result in a reactor trip but could increase the initiating event frequency of the total loss of the support system. See Section 11 for guidance on evaluating failures of support system components.
- A degraded condition that could increase the frequency of an initiating event (e.g., excessive pipe wall thinning without loss of function).
- For SDP evaluations where a PD did not cause a reactor trip, but contributed to a consequential initiating event (e.g., LOOP event) resulting in a reactor trip, is evaluated via a condition analysis.

Note that a Bayesian update of the initiating event frequency using the observed initiating event over a specific period should not be used for treatment of initiating events in ECA because the

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

[40] The term "mutually exclusive" in this case means that the affected component(s) of the degraded condition(s) are not queried by the applicable event tree and fault tree logic for the initiating event that occurred.

goal is to estimate the risk significance of the actual occurrence of an event, and the Bayesian update produces a change in the initiating event frequency that reflects the occurrence of the initiating event over a certain period, which is a different calculation. Furthermore, a Bayesian update assumes that the prior distribution and the plant-specific data are consistent; the fact that the initiating event was caused by a failure, which is assumed to cause a significant increase in the frequency of the initiating event, invalidates this assumption

8.2 Case 1 – Initiating Event Only

For this case, an initiating event with a subsequent reactor trip occurs with no concurrent degraded conditions during the event. For SDP evaluations, the PD must be the cause of the initiating event. For ASP and MD 8.3 analyses, a PD does not have to be associated with the initiating event.

8.2.1 Calculate the CCDP

Analysts need to calculate the CCDP by setting the probability of the observed initiating event (e.g., general transient, loss of MFW, loss of safety bus transient) to 1.0 and the probabilities of all other initiating events to 0. For ASP and MD 8.3 analyses, the final metric is the CCDP.[41]

8.2.2 Calculate the ΔCDF$_{ave}$ (SDP only)

For SDP evaluations, the base CDP of the applicable initiating event needs to be subtracted from the CCDP to calculate the ΔCDP using the following formula:

$$Base\ CDP_{Initiating\ Event} = Base\ CDF_{Initiating\ Event} \times \left(\frac{1\ year}{8760\ hours}\right) \times 24\ hours$$

The ΔCDP is then multiplied by one inverse year (yr^{-1}) to convert it to a ΔCDF$_{ave}$, which is the metric used for the SDP evaluations. Figure 8-1a and Figure 8-1b provide the CDP versus time and CDF versus time for Case 1.

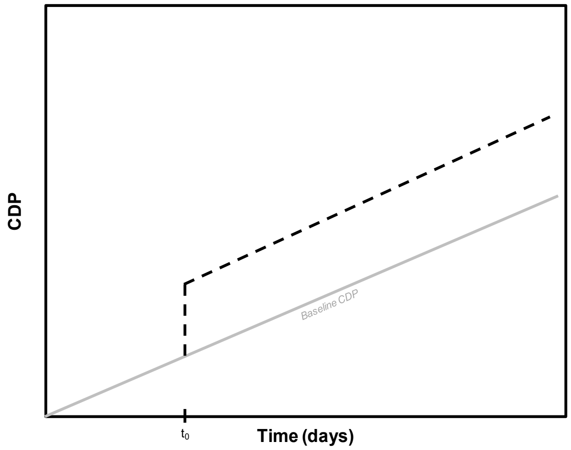


Figure 8-1a. CDP vs. Time for Case 1

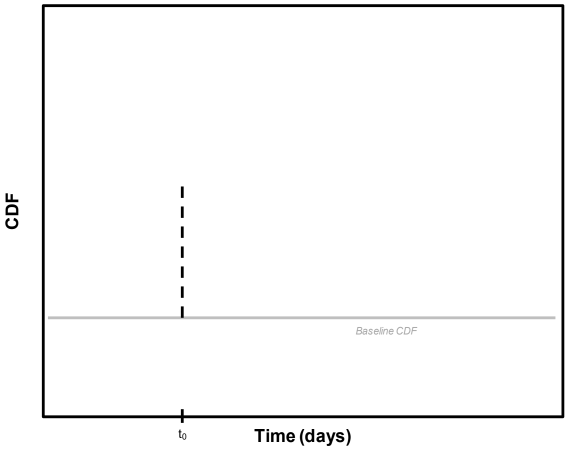


Figure 8-1b. CDF vs. Time for Case 1

[41] CCDP is also the metric used for SDP evaluations of shutdown initiating events (e.g., losses of shutdown cooling).

The plot of CDP vs. time (Figure 8-1a) shows a line representing the CDP vs. time prior to the initiating event, at t_0 a “spike” in CDP accumulates due to an initiating event with subsequent reactor trip, and then the CDP returns to the same slope as the baseline CDP following the initiating event (t_0).[42],[43] A plot of CDF vs. time (Figure 8-1b) shows a horizontal line (equal to the baseline CDF), with Dirac delta function (or “spike”) at t_0 when the reactor trip occurs. After the initiating event occurs, the CDF returns to equal the baseline CDF. The CDP is approximately the integral of CDF over time. At the point where the initiating event occurs (t_0), the integral is equal to the CCDP multiplied by the integral of the delta function, which is numerically equal to the CCDP.

8.3 Case 2 – Initiating Event and Concurrent Degraded Condition(s)

For this case, an initiating event with a subsequent reactor trip occurs along with concurrent degraded condition(s). For SDP evaluations, the same PD must be the cause of the initiating event and the concurrent degraded condition(s).[44] For ASP and MD 8.3 analyses, a PD does not have to associated with the initiating event and/or the degraded condition(s). This case involves the comparison of the risk impacts of the initiating event with the concurrent degraded condition (initiating event analysis) and the degraded condition by itself (condition analysis). To avoid double counting, the analysis result with the highest risk significance is documented for the record.

8.3.1 Calculate the CCDP for the Initiating Event

Analysts need to calculate the CCDP by setting the probability of the observed initiating event (e.g., general transient, loss of MFW, loss of safety bus transient) to 1.0 and the probabilities of all other initiating events to 0. In addition, the basic event(s) associated with the degraded condition(s) should be set to TRUE.[45] For ASP and MD 8.3 analyses, the final metric is the CCDP.

8.3.2 Calculate the ΔCDF_{ave} for the Initiating Event (SDP only)

For SDP evaluations, the base CDP of the applicable initiating event needs to be subtracted from the CCDP to calculate the ΔCDP using the formula shown in Section 8.2.2. The ΔCDP is then multiplied by one inverse year (yr^{-1}) to convert it to a ΔCDF_{ave}, which is the metric used for the SDP evaluations.

8.3.3 Calculate the ΔCDP or ΔCDF_{ave} of the Degraded Condition(s)

Analysts need to calculate the ΔCDP by of the degraded condition(s) by setting the appropriate basic events to TRUE for the applicable exposure time(s). For ASP and MD 8.3 analyses, the

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

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

[44] In the SDP, a PD that causes an initiating event with subsequent reactor trip will be evaluated separately from other PDs revealed during the event. The guidance of IMC 0609 and IMC 0308 apply to defining PDs.

[45] Basic events associated with failed components should be set to TRUE to ensure the potential for CCF is estimated. Basic event(s) of failed component(s) should only be set to 1.0 if a deviation of key CCF principles is identified (see Section 5.8.2 for additional information).

final metric is the ΔCDP. For SDP evaluations, the ΔCDP is then multiplied by one inverse year (yr^{-1}) to convert it to a ΔCDF_{ave}. The overall final analysis result will be the higher $CCDP/\Delta CDF_{ave}$ between the initiating event analysis and the $\Delta CDP/\Delta CDF_{ave}$ from the condition analysis.

8.4 Case 3 – Initiating Event and Mutually Exclusive Degraded Condition(s) (SDP Only)[46]

For this case, a PD causes an initiating event with subsequent reactor trip. In addition, the same PD also causes degraded condition(s) that are mutually exclusive of the initiating event.[47] The exposure time of the degraded conditions may or may not overlap with when the reactor trip occurred. However, the unavailable SSC is not required for mitigation of any of the initiating event sequences. This case only applies for SDP evaluations.

Case 2 involves three calculations: (1) ΔCDF_{ave} estimation associated with just the initiating event, (2) ΔCDF_{ave} estimation associated with just the degraded condition(s) for the applicable exposure time(s), and (3) the sum of the two results.

8.4.1 Calculate the ΔCDF_{ave} for the Initiating Event

For the initiating event analysis, analysts must first calculate the CCDP by setting the probability of observed initiating event (e.g., general transient, loss of MFW, loss of safety bus) to 1.0 and the probabilities of all other initiating events to 0. The base CDP of the applicable initiating event needs to be subtracted from the CCDP to calculate the ΔCDP using the formula shown in Section 8.2.2. The ΔCDP is then multiplied by one inverse year (yr^{-1}) to convert it to a ΔCDF_{ave}.

8.4.2 Calculate ΔCDF_{ave} for the Degraded Condition(s)

For the condition analysis, analysts must first calculate the ΔCDP by selecting the basic event(s) associated with the degraded condition(s) to TRUE for the applicable exposure time(s). The ΔCDP is then multiplied by one inverse year (yr^{-1}) to convert it to a ΔCDF_{ave}.

8.4.3 Calculate Total ΔCDF_{ave}

Calculate the total ΔCDF_{ave} by summing the ΔCDF_{ave} for the initiating event and the ΔCDF_{ave} for the degraded condition. Figure 8-2a and Figure 8-2b provide the CDP versus time and CDF versus time for Case 3. From t_0 to t_1 Case 3 is identical to Case 1; however, the same PD that caused an initiating event with subsequent reactor trip at t_0 also caused a degraded condition from t_1 to t_2 (i.e., Δt). The failed component was restored at t_2.

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

[46] This case only applies for SDP evaluations. MD 8.3 or ASP analysis requires degraded condition(s) to be concurrent with the initiator's PRA mission time (i.e., within 24 hours following the reactor trip).

[47] The term "mutually exclusive" used in this case means that the applicable component(s) affected by the degraded condition(s) are not queried in the applicable event tree and fault tree logic and, therefore, the risk impact will not be accounted for in the initiating event analysis.

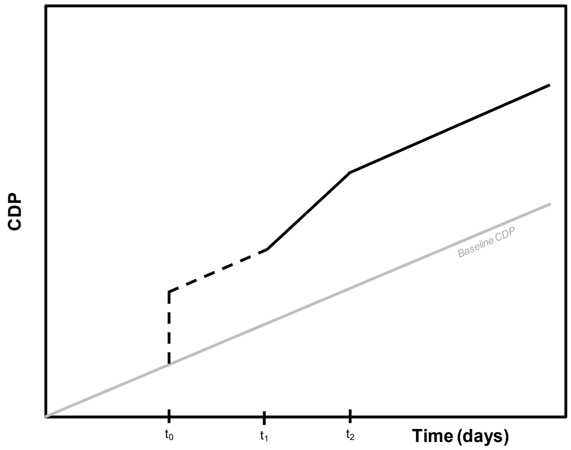


Figure 8-2a. CDP vs. Time for Case 2

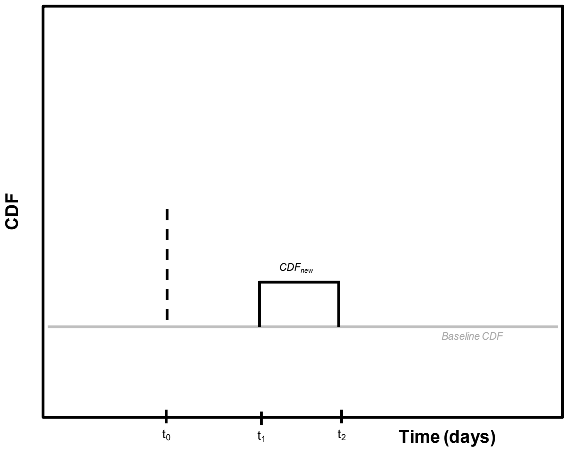


Figure 8-2b. CDF vs. Time for Case 2

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

These plots show an example of Case 3 where the initiating event and condition do not overlap, and the deficiencies associated with the initiating event and condition were fixed at different times (t_0 and t_2, respectively). Other variations of this case are possible, such as the condition starting at a time before the reactor trip and then corrected after the reactor trip.

9 HRA

9.1 Purpose

The purpose of this guide is to address the application of HRA methods in SDP, ASP, NOED, or MD 8.3 assessments. These applications require the analysts to perform analyses of sufficient quality to support regulatory decision-making in Reactor Oversight Process and incident response activities. The HRA guidance presented here provides best practices in HRA to enable the NRC staff to make timely decisions whose quality is adequate for those processes. However, this guidance may not constitute acceptable positions in all regulatory applications (e.g., license amendment requests). In the development of this guidance, the staff has referred to various sections of reports issued by the NRC, national laboratories, and industry to present best practices that would result in realistic results and enable achieving technical consistency and stability of regulatory decisions. However, this strategy does not constitute unconditional endorsement of those references for all regulatory applications.

Basic events representing human actions required to mitigate initiating events are contained in the SPAR models. The existing HEPs in the SPAR models are industry average values based on cutset level reviews performed by INL. This approach is similar to the use of industry-average data for component reliability and availability parameters in the SPAR models. SAPHIRE includes the ability to quantify HEPs using NUREG/CR-6883, “SPAR-H Human Reliability Analysis Method,” (ML15142A653). The industry average HEP values used in the SPAR models are presented in the SPAR-H format, but SPAR-H was not used to derive the values.

An NRC risk analyst may need to re-quantify a HFE already contained in the model and/or the analyst may need to add an HFE(s) based on the specifics of the risk analysis.[48] Human actions may be quantified using SPAR-H. In 2022, the NRC documented a new HRA method in NUREG-2256, “Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA),” (ML22300A117). Human actions may also be quantified for event assessments using IDHEAS-ECA.

In light of the importance of operator actions on the risk significance of some events, the analyst should consult an HRA expert and document the technical basis for adding the HFE [if an analyst decides to add new HFE(s)].[49]

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

[49] An HRA expert should have training and experience with the particular application of the HRA method being used. Definition is referenced from NUREG-1489, “A Review of NRC Staff Uses of PRA,” (ML063540593).

9.2 Key Aspects of the SPAR-H Method

9.2.1 Background

The SPAR-H framework decomposes the HEP into contributions from diagnosis failures and action failures. In addition, the SPAR-H quantification process accounts for the influence of eight PSFs. In 2011, INL/EXT-10-18533, “SPAR-H Step-by-Step Guidance,” (ML112060305), was developed to provide guidance for analysts when plant-specific information is available (e.g., during ECAs), which supplements the general guidance provided in the NUREG/CR-6883. A summary of the key steps of using SPAR-H are provided below.

9.2.2 Step 1: Categorizing the HFE as Diagnosis and/or Action

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

9.2.3 Step 2: Evaluate the PSFs

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

- Available Time
- Stress/Stressors
- Complexity
- Experience/Training
- Procedures
- Ergonomics/Human-Machine Interface
- Fitness for Duty
- Work Processes

INL/EXT-10-18533 provides detailed information on how an analyst should assign the appropriate PSF level once a particular PSF is determined to be a “performance driver.” In addition, an analyst should only include assessment of multiple PSFs if there is reason to believe that each of the respective PSFs is a separate performance driver in its own right, and not merely as a side effect of one of the other PSFs (i.e., "double counting").[50]

9.2.4 Step 3: Calculate PSF-Modified HEP

Once the PSF levels have been assigned, then the final HEP is simply the product of the nominal HEP and the PSF multipliers. When Diagnosis and Action are combined into a single HFE, the two HEPs are calculated separately and then summed to produce the composite HEP. Mathematically, it is possible to have a value exceeding 1.0; however, if the two probabilities are small, then the rare-event approximation (i.e., the simple arithmetic sum) is acceptable. In the event that a combined Diagnosis and Action HEP approaches or exceeds 1.0, the following equation should be applied:

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

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

9.3 Key Aspects of the IDHEAS-ECA Method

9.3.1 Background

IDHEAS-ECA is intended to apply to the same situations modeled by existing HRA methods (e.g., NPPs internal events while at-power) and situations that are beyond the scope of existing methods (e.g., external events, low power and shutdown events, and events for which FLEX equipment is used). IDHEAS-ECA is based on the HRA methodology in NUREG-2198, "The General Methodology of an Integrated Human Event Analysis System (IDHEAS-G)," (ML21127A272). IDHEAS-ECA models HFEs using five macrocognitive functions. These macrocognitive functions are based on the cognitive basis for HRA, which was published as NUREG-2114 and are described as follows:

1. Detection is noticing cues or gathering information in the work environment.
2. Understanding is the integration of pieces of information with a person's mental model to make sense of the scenario or situation.
3. Decision-making includes selecting strategies, planning, adapting plans, evaluating options, and making judgments on qualitative information or quantitative parameters.
4. Action execution is the implementation of the decision or plan to change some physical component or system.
5. Interteam coordination focuses on how various teams interact and collaborate on an action.

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

The failure of a macrocognitive function is defined as the cognitive failure mode (CFM). The probability of an HFE (i.e., HEP) is affected by the scenario context in which the action occurs. The context describes the conditions that challenge or facilitate human performance. IDHEAS-ECA uses performance influencing factors (PIFs) and PIF attributes to model the context. The IDHEAS-ECA software tool should be used to facilitate documentation and calculation of the HEP.

The IDHEAS-ECA method provides step-by-step guidance for analyzing a human action and its context. IDHEAS-ECA is an 8-step process, as summarized below:

1. Analyze the scenario. Analyzing an event includes developing the scenario narrative and timeline, determining the scenario context, and identifying the HFEs.
2. Analyze the HFE. This includes defining the HFE, analyzing the tasks within the human action, and identifying the critical tasks for HEP quantification. The definition of the HFE describes the failure of the human action, its link to the affected systems in the PRA model, and the timeline.
3. Model the failure of critical tasks in an HFE. This includes characterizing the critical task and selecting the applicable CFMs of the critical task. Characterization of a critical task means specifying the conditions relevant to the critical task that can challenge or facilitate human performance. Any critical task can be achieved through one to all five macrocognitive functions.
4. Assess the PIFs applicable to every CFM. The PIFs represent the context of the HFE and facilitate quantification of the HEP. A PIF attribute is an assessable characteristic of a PIF and describes a way the PIF challenges the macrocognitive functions of a critical task and thus increases the likelihood of error in the macrocognitive functions.
5. Calculate the probability of failure due to the CFMs (P_c). P_c is calculated as the probabilistic sum of the HEPs of all the CFMs of the critical tasks, which are based on the PIF attributes assessed in Step 4.
6. Calculate the probability of failure due to the uncertainty in time available and time required to perform the action (P_t).
7. Calculate the overall HEP. The overall HEP is the probabilistic sum of P_c and P_t. That is, Overall HEP = 1 − (1−P_c) (1−P_t).
8. Analyze uncertainties in the HRA, perform sensitivity and dependency analyses, and document the results.

Research Information Letter (RIL) 2024-17, “IDHEAS-ECA Evaluations of SPAR Model Human Failure Events,” (ML24352A019) provides several examples IDHEAS-ECA evaluation of base SPAR model HFEs.

9.4 Minimum HEP for Single HFE

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

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

In order to ensure consistent implementation of SDP, ASP, and MD 8.3 analyses, the minimum recommended HEP (i.e., lower bound) for a single HFE is 10^{-5}. NUREG-1792 states that "typical post-initiator HEPs are expected to be in the range of 0.1 to 10^{-4}).[51] In the event the analyst concludes that use of the lower bound 10^{-5} leads to an overly conservative conclusion, document the technical basis for deviating from the lower bound and have it validated by an HRA expert. Criteria that can justify a single HEP as low as 10^{-6} (as suggested by EPRI Report 1021081, "Establishing Minimum Acceptable Values for Probabilities of Human Failure Events: Practical Guidance for PRA,") are as follows:[52]

– Well-practiced,

– Familiar responses with expansive time to respond,

– Numerous indications (cues) of the need for action,

– Procedural guidance and training that leads to monitoring of plant status to assess the efficacy of response, thus allowing opportunity for self-correction, and

– Low workload (i.e., no distractions).

9.5 Analysis of Dependencies

9.5.1 Determination of Dependency

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

It is expected that the qualitative analysis and resulting context and operational story should help to identify the existence of compelling reasons for dependence. The analyst should be on the lookout for situations in which operators develop an incorrect mindset about the situation and identify ways in which that mindset can be corrected to break dependence. Analysts should

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

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

review the situation and context carefully and consider, for example, the following factors which may allow for an opportunity to minimize or break dependence:

- Time (to allow forgetting and emptying of working memory),[53].
- Location (introducing new information, potentially interrupting the erroneous mindset),
- Different people or crew (allows for new mindset to develop), and
- Cues (stimulate the human to think differently).

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

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

9.5.2 Accounting for Dependence

In PRA and HRA, dependence can be accounted for in the following ways.

9.5.2.1 Common PSF Adjustment

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

9.5.2.2 THERP Dependency Table

In determining the level (i.e., degree) of dependence, SPAR-H adapts from Technique for Human Error Rate Prediction (THERP) the factors of same person/crew, close/not-close in time, same/different location, and presence/absence of additional cues.[54] SPAR-H also adapts the same dependence levels used in THERP: zero, low, moderate, high, and complete. The dependence level table in SPAR-H was designed to identify situations in which there is likely to

[53] The analyst must consider time available to implement recovery actions against the time required to determine the influence of this factor on dependency. For example, whereas 10 minutes may have no impact, one or more shift turnovers may have a significant influence on dependency.

[54] THERP is documented in NUREG/CR-1278, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications," (ML071210299).

be a commonly held misperception of the scenario. To maintain consistent application of guidance, analysts should document the basis and/or assumptions for any deviations. If such deviations are likely to contribute to significant regulatory outcomes, the analyst should request an independent validation of the assumptions by an HRA expert.

9.5.2.3 IDHEAS Dependency Method (IDHEAS-DEP)

IDHEAS-DEP is documented in RIL 2021-14, "Integrated Human Event Analysis System Dependency Analysis Guidance (IDHEAS-DEP)," (ML21316A107). IDHEAS-DEP includes two levels of dependency analysis, screening and detailed, for use with pairs of HEPs. A screening analysis can be performed for pairs of HFEs with HEPs that were calculated using any HRA method. A detailed analysis is intended for use with HEPs that were calculated using IDHEAS-ECA. IDHEAS-DEP begins with a predetermination analysis which evaluates whether the HEP pair is independent, completely dependent, or any of five dependency relationships exist. The five dependency relationships are as follows:

1. Functions or Systems – this relationship is evaluated when the HFE pair are performed using equipment that has the same function or is part of the same system.
2. Time Proximity – this relationship is evaluated when the HFE pair are performed close in time or the cues for the HFEs are received close in time.
3. Personnel – this relationship is evaluated when both HFEs are performed by the same personnel.
4. Location – this relationship is evaluated when the HFE pair are performed in the same location.
5. Procedures – this relationship is evaluated when the HFE pair are performed in the same location.

If a dependency relationship exists, the impact of the relationship is assessed using a screening and/or detailed analysis. The analyst can perform both a screening and detailed analysis, or just one of the two, depending on how much information the analyst has about the HEP pair and how detailed a result is desired.

9.5.2.4 Apply Joint HEP for Multiple HFEs

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

EPRI Report 1021081 provides a more detailed approach in determining the level of dependence between HFEs and applying minimum joint probabilities. Based on the determination of the level of dependence, an analyst may assign a joint HEP of 10^{-5} (low dependence) or 10^{-6} (very low dependence).[55] In addition, the report states that, “if the criteria for independent HFEs are met, it should not be necessary to employ an alternative minimum value rather than the one calculated.”

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

- Are the HFEs related to the same critical safety function?
- The amount of time that separates the actions.
- The level of operator workload.
- The quality of instrumentation and procedures.
- Is the need for each HFE indicated by separate/multiple cues?
- Are the crew and plant being monitored independently by the shift supervisor and/or shift technical assistant?

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

9.5.2.5 SDP-Specific Guidance

To minimize the subjectivity in SDP analyses, an analyst should consult an HRA expert to determine if a minimum joint HEP of lower than 10^{-5} should be used. Some questions that the analyst must discuss with the HRA expert prior to determining whether a minimum joint HEP lower than 10^{-5} can be used are:

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

If use of a minimum joint HEP of less than 10^{-5} is justified, the rationale must be documented in the risk evaluation.

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

10 LOOP Events

10.1 Purpose

This section provides guidance for risk analysis of LOOP events. This guide supplements the guidance provided in Section 8 of this handbook. The guidance provided in this section is primarily for SDP, MD 8.3, and ASP assessments.

10.2 Scope

The scope of this guide includes analysis of LOOP and partial LOOP events. These events may or may not be associated with an initiating event (i.e., reactor trip).

10.3 Definitions

10.3.1 LOOP Event

NUREG/CR-6890, "Reevaluation of Station Blackout Risk at Nuclear Power Plants," (ML060200477) defines a LOOP event as:

> *The simultaneous loss of electrical power to all plant safety buses, requiring all emergency power generators to start and supply power to the safety buses. The nonessential buses may also be deenergized as a result of this.*

Most LOOPs result in the loss of offsite power to the nonsafety buses (in addition to the safety buses) and a subsequent reactor trip. LOOP events that do not result in a reactor trip are modeled via SSC electrical dependencies within the applicable fault tree logic.

10.3.2 LOOP Initiating Event

NUREG/CR-6890 defines a LOOP initiating event as:

> *A LOOP occurring while a plant is at power and also involving a reactor trip. The LOOP can cause the reactor to trip or both the LOOP event and the reactor trip can be part of the same transient.*

There are the following four types of LOOP initiating events (based on cause or location):

- Plant Centered
- Switchyard Centered
- Grid Related
- Weather Related

Table 10-1 provides revised definitions for these four LOOP types taken from INL/RPT-24-79969, "Analysis of Loss-of-Offsite-Power Events 2023 Update". The SPAR models include separate events trees for these different LOOP initiating event types. The key differences in the modeling of the different LOOPs are differences in the initiating event frequencies and the LOOP non-recovery probabilities.

Table 10-1. LOOP Type Definitions

LOOP Class	Definition
Plant Centered	*A LOOP event in which the design and operational characteristics of the NPP unit itself play the major role in the cause and duration of the LOOP.* Plant-centered failures typically involve hardware failures, design deficiencies, human errors, and localized weather-induced faults (e.g., caused by lightning). The line of demarcation between plant-centered and switchyard-centered events is the NPP main and station power transformers' high-voltage terminals. Both transformers are considered part of the switchyard.
Switchyard Centered	*A LOOP event in which the equipment or human-induced failures of equipment in the switchyard play the major role in the LOOP.* The line of demarcation between switchyard-centered events and grid-related events is the point where the transmission lines leave the switchyard.
Grid Related	*A LOOP event in which the initial failure occurs in the interconnected transmission grid that is outside the direct control of plant personnel.* Failures that involve transmission lines within the site switchyard are usually classified as switchyard-centered events if plant personnel can take actions to restore power when the fault is cleared. However, the event should be classified as grid related if the transmission lines fail from voltage or frequency instabilities, overload, or other causes that require restoration efforts or corrective action by the transmission operator.
Weather Related	*A LOOP event caused by severe or extreme weather, in which the weather was widespread, not just centered on the site, and capable of major disruption. Severe weather is defined as weather with forceful and non-localized effects.* An example is storm damage to transmission lines instead of just debris blown into a transformer. This does not mean that the event had to result in widespread damage, just that the potential existed. Examples of severe weather include thunderstorms, snow, and ice storms. Lightning strikes, though forceful, are normally localized to one unit, and so are coded as plant centered or switchyard centered. Hurricanes, strong winds greater than 125 miles per hour, and tornadoes are examples of extreme-weather-related LOOPs.

10.3.3 LOOP No-Trip Event

NUREG/CR-6890 defines a LOOP no-trip event as:

> *LOOP occurring while a plant is at power but not involving a reactor trip.*

10.3.4 Partial LOOP

NUREG/CR-6890 defines a partial LOOP event as:

> *The loss of electrical power to at least one but not all unit safety buses that requires at least one emergency power generator to start and supply power to the safety bus(es).*

As is the case for LOOP events, partial LOOP events may or may not result in a subsequent reactor trip (depending on whether offsite power is lost to the nonsafety buses). Most SPAR models do not have partial LOOP event trees.[56] Therefore, the partial LOOP initiating events

[56] Most SPAR models have loss of safety AC bus event trees; however, these initiating events assume the bus has failed. Therefore, the use of these event trees is not appropriate for the modeling of partial LOOPs in most cases.

need to be modeled using the appropriate transient event tree (e.g., transient, loss of feedwater, loss of condenser heat sink) and the appropriate LOOP flag events or electrical SSC basic events located within the applicable fault trees. Partial LOOP events that do not result in a reactor trip are modeled using only the appropriate LOOP flag events or electrical SSC basic events.

10.3.5 Consequential LOOP

NUREG/CR-6890 defines a consequential LOOP event as:

> *A LOOP initiating event in which the LOOP is the direct or indirect result of a plant trip. For example, the event is consequential if the LOOP occurred during a switching transient (i.e., main generator tripping) after a unit trip from an unrelated cause. In this case, the LOOP would not have occurred if the unit remained operating.*

Consequential LOOPs are included in most SPAR models via the OEP top event/fault tree, which is queried in applicable event trees where the initiating event could result in a consequential LOOP. For the SPAR models that include OEP fault tree in their event trees, some initiating events (e.g., medium and large LOCA) have a deactivated LOOP event tree transfer to ensure the proper modeling of the event. Note that the fault trees for the SSC electrical support will account for consequential LOOPs as well.

10.4 Industry-Wide LOOP Non-Recovery Curves

The probabilities of non-recovery of offsite power to the first safety bus for various recovery times for each LOOP types were originally provided in NUREG/CR-6890. These probabilities have been updated as part of the periodic LOOP updates, which are provided on the Reactor Operational Experience Results and Databases LOOP Web Page.[57] Industry-wide LOOP non-recovery curves are generally used for condition assessments (e.g., failure of an EDG) or preliminary analyses of a LOOP initiating event where event details are not initially well known. Note that each SPAR model has several offsite power non-recovery basic events based on key times for different accident sequences that are applicable to the specific plant design. These non-recovery events are mostly associated with postulated SBO scenarios included in the SBO and SBO-ELAP event trees.[58] Some examples of these key times include:

– Time to core uncovery given a LOOP initiating event, subsequent (postulated) SBO, and failure of decay heat removal (AFW and reactor core isolation cooling (RCIC)/high-pressure coolant injection (HPCI)).

– Time to core uncovery given a LOOP initiating event, subsequent (postulated) SBO, and subsequent LOCA due to failure of the reactor coolant pump (RCP) seals or stuck-open relief valve(s).

[57] The non-recovery time distributions are updated in the biannual LOOP updates. However, the non-recovery probabilities used in the SPAR models are provided in the LOOP update from the year the SPAR model update occurred. For example, the current SPAR models use non-recovery probabilities derived from the distributions in the INL/EXT-21-64151, “Analysis of Loss of Offsite Power Events 2020 Update,” which was the year the of last SPAR model parameter update.

[58] Some LOOP event trees for PWRs include offsite power non-recovery event(s) given a LOCA and successful high-pressure injection or failure of decay heat removal with successful feed and bleed cooling. The recovery of offsite power would allow operators to cooldown/depressurize the reactor coolant system (RCS) to allow for initiation of shutdown cooling mode of RHR in lieu of initiating cold-leg recirculation.

- Normal SBO coping time (i.e., normal depletion time of safety-related batteries).
- Extended SBO coping time given successful deep DC load shed.

10.5 FLEX Mitigating Strategies Modeling

The SPAR models include the FLEX mitigating strategies in the SBO-ELAP events trees. Specifically, accident sequences where there is no LOCA and initial decay heat removal (AFW or RCIC) is successful are transferred to the SBO-ELAP event tree, which includes credit for the Phase 2 FLEX mitigating strategies. The FLEX equipment basic events use the reliability parameters provided in Pressurized Water Reactor Owner's Group 18042-NP, "FLEX Equipment Data Collection and Analysis," (ML22123A259). Analysts must currently activate this credit for ECAs (i.e., the FLEX mitigation strategy modeling is deactivated in the base SPAR models).[59]

The existing SBO-ELAP event tree structure in each SPAR model is a generic event tree based on an initial high-level understanding of implementing the Phase 2 FLEX mitigating strategies for each plant type (i.e., BWR or PWR). The current modeling provides a good starting point for crediting the FLEX mitigation strategies; however, analysts should review the licensees' final integrated plan (FIP) to determine if modifications to the SBO-ELAP event tree and/or FLEX fault trees is needed.[60] The following subsections provide a brief discussion of some key modeling assumptions analysts should consider to determine if model revisions are needed.

10.5.1 Offsite Power Recovery After Battery Depletion

Most SPAR models currently credit offsite power recovery after the safety-related batteries have been depleted. This credit may not be appropriate because safety-related DC power for breaker manipulations is typically required to realign offsite power to safety buses. In addition, additional DC powers sources (e.g., switchyard batteries) may be required to restore offsite power for certain LOOP types. Some licensees may also strip power from switchyard breakers, as part of the deep load shed, that are required to restore offsite power to a safety bus. Analysts should not credit offsite power recovery if required DC power sources are unavailable to support realignment actions (e.g., closing of breakers) unless alternative methods for performing the required actions are available, proceduralized, and a part of the operator training program.

10.5.2 EDG Repair

The SPAR models currently credit EDG repair in the SBO and SBO-ELAP event trees. Specifically, the SBO event tree queries EDG repair (along with offsite power recovery) at key plant-specific times (examples of these key SBO times are provided Section 10.4.1) and the SBO-ELAP event tree includes credit for EDG repair in the 24- and 72-hour offsite power recovery fault trees. However, this credit may not be appropriate after ELAP has been declared at most NPPs because (at minimum staffing levels) personnel sent to troubleshoot the failed EDGs are typically reassigned to implement the FLEX mitigation strategies. In addition, many plants strip loads during the deep DC load shed that are required to start and/or run the EDGs.

[59] The FLEX credit must be activated in the base SPAR model for condition assessments. Credit for the FLEX mitigating strategies will be activated in the base SPAR models in the future, perhaps as early as the next data update to be completed in 2026.

[60] The SBO-ELAP event trees in some base SPAR models have already been revised based on a review of the specific plants' final integrated plan (FIP).

Analysts should not credit EDG repair after ELAP declaration unless the licensee has the required personnel (at minimum staffing levels) to continue to troubleshoot the failed EDG(s) and has appropriate training and procedures to restore required loads for EDG operation.

10.5.3 N+1 FLEX Equipment

The current SPAR models do not credit the N+1 FLEX equipment, which could be overly conservative for some plants and/or scenarios. Analysts should review plant information to determine if sufficient time is available to transport, install, and start the N+1 FLEX equipment given the failure of the N train. Note that N+1 FLEX equipment may have alternative connection strategies, which would typically preclude crediting given time constraints.

10.5.4 LOCAs or Failures of Decay Heat Removal

The SPAR models currently do not credit the FLEX mitigation strategies for postulated SBOs with a subsequent LOCA or failure of decay heat removal (AFW or RCIC) because it is expected that there would be insufficient time to transport, connect, and start the required FLEX equipment prior to core damage for these scenarios. In addition, most licensee FIPs state that the FLEX mitigation strategies are not able to prevent core damage in these scenarios. This modeling assumption could be conservative for plants with permanently installed FLEX equipment. If a plant has permanently installed FLEX equipment that could prevent core damage, analysts should review the plant information (e.g., procedures, timing information, etc.) to determine if FLEX credit should be provided for these scenarios.

10.5.5 RCS Makeup (PWRs only)

The PWR SPAR models require RCS makeup to be initiated for the plant to reach a safe/stable end state. This is in alignment with most (if not all) PWR licensee FIPs requiring RCS injection to provide inventory makeup for leakage from RCP seals and to provide additional shutdown margin. This modeling assumption could be conservative for plants that have installed advanced RCP seals that limit leakage to less than 1 gpm. If this modeling assumption is to be changed, analysts should ensure that reflux cooling will not be reached within (or closely after) the PRA mission time (i.e., 24 hours). In addition, analysts should verify that additional shutdown margin is not required.

10.5.6 RCIC Failure (BWRs only)

Most current BWR SPAR models do not credit the FLEX mitigation strategies if RCIC has failed but HPCI or high-pressure core spray (HPCS) is successful, which could be overly conservative. Most BWR licensee FIPs are written within the context that RCIC is successful and are mostly silent regarding whether RCIC and HPCI/HPCS are interchangeable in providing early decay heat removal and inventory control during an ELAP. If credit for the FLEX mitigation strategies given successful HPCI/HPCS operation and the failure of RCIC, analysts should review plant procedures (e.g., deep load shed procedure) to ensure continued operation of HPCI/HPCS is supported.

10.6 Analysis Types

The following subsections provide information on what type ECA should be performed for different LOOP events and key considerations. Table 10-2 provides a list of information typically needed to perform ECAs LOOP events.

Table 10-2. Information Typically Needed for the Risk Analysis of LOOP Events

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

- □ Equipment out-of-service for test or maintenance
- □ Electrical power lineups (note any unusual lineups due to ongoing maintenance or surveillance testing)
- □ RCP seal type (PWRs)
- □ Pressurizer PORV block valves open/closed during power operation (PWRs)
- □ Power history (time of last plant shutdown)

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

- □ Fault that caused LOOP
  - o Location of fault(s)
  - o Cause of fault(s)
- □ Restoration of power to first owner-controlled switchyard breaker:
  - o Important actions taken by the plant and outside organizations to recover power
  - o Time when power from the grid stabilized
  - o Time when the control room was informed
- □ Status of alternate power sources, such as black-start equipment and crossties (see note 1):
  - o Equipment starts and loads
  - o Time when equipment was secured
  - o Observed problems (e.g., trips, reduced performance)
- □ Status of emergency power sources (e.g., diesel generators):
  - o Equipment starts and loads
  - o Time when equipment was secured
  - o Observed problems (e.g., trips, reduced performance)
- □ Depletion of plant and switchyard batteries, if any, and what DC loads are supported
- □ Status of safety systems (e.g., AFW, high-pressure injection):
  - o Automatic actuations
  - o Manual actuations
  - o Time when equipment was secured
  - o Observed problems (e.g., trips, reduced performance)
- □ Status of BOP systems:
  - o Power lost and recovered to non-safety BOP buses
  - o Availability of MFW and primary conversion system
  - o Loss of condenser heat sink
  - o Main steam isolation valve closure(s)
  - o Loss of MFW pumps
  - o Loss of instrument air
- □ Primary SRV(s) and/or PORVs (PWR) demands (include each demand, if possible)
- □ Equipment failures and performance issues observed during the event:
  - o Switchyard
  - o In-plant electrical distribution system
  - o Safety systems
  - o Reactor coolant pump seals (PWR)
- □ Failed or out-of-service equipment recovered during the event
- □ Recovery of offsite power to each safety bus
- □ Operator performance issues

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

- ☐ Availability of offsite power to carry electrical loads to mitigate reactor coolant pump seal leakage (PWR) or stuck open safety/relief valve LOCA and to bring the plant to cold shutdown:
  - o Actual time when offsite power was stable (voltage and frequency)
  - o How was this time determined?
  - o Estimated time when control room staff knew that offsite power was stable to carry critical electrical loads
- ☐ Delineation of owner-controlled breakers in the switchyard and black-start capability (most can be found in plant procedures):
  - ○ Plant control boundary
  - ○ Breaker controls and start capability in the control room
  - ○ Communications needed with outside organizations including another control room of a multi-unit site
  - ○ Availability of outside organizations needed to support power recovery 24 hours per day,7 days a week
- ☐ Steps taken to recover offsite power to the first safety bus including control room and local actions
- ☐ Breaker alignments
  - o Actual path taken to bring in offsite power to safety buses
  - o Alternative success paths to bypass the electrical fault
- ☐ Estimate of the earliest time when offsite power could have been restored to the first safety bus.
- ☐ Operator and equipment performance issues

4. ***Equipment Initiation and Recovery –*** Assessment of the actuation or recovery of risk-important systems as determined by preliminary SPAR model analysis:[61]

- ☐ Typical systems that are important to risk during LOOP and SBO sequences include:
  - ○ Offsite power to the first safety bus (refer to Item 3)
  - ○ Start and load of alternate power sources
  - ○ Failed equipment
  - ○ Equipment in test or maintenance
  - ○ MFW (TDP or MDP)
  - ○ Condenser heat sink
  - ○ Instrument air
- ☐ Assessments of the recovery of risk significant system(s) should be performed in the context of the applicable core damage sequence, even if the system was not initiated or recovered during the actual LOOP event. Each assessment should include
  - ○ Determination whether the recovery is creditable within the component PRA mission time (usually 24 hours) given the nature of the equipment damage.
  - ○ List of operator actions, including diagnostic actions and repair/recovery actions inside and outside the control room.
  - ○ Time needed to complete the action, including upper and lower bounds. In some cases, the actual time observed during the event may be a reasonable approximation for the mean/average time, excluding the time taken for paperwork.
  - ○ Availability of necessary information for worst case scenarios:
    - ▪ Procedures
    - ▪ Plant staffing with the necessary skills
    - ▪ Staffing of key external support organizations (e.g., transmission dispatch operators)
    - ▪ Tools

[61] This information will be used in the HRA to evaluate the applicable PSFs/PIFs.

- ▪ Lighting; electrical power for tools
- ▪ Spare parts

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

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

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

☐ Crossties between plants (refer to item 6, below, for criteria for crediting crossties):
- ○ Shared EDG
- ○ Crosstie of the Division III (high-pressure core spray) bus to another bus (BWR 5/6)
- ○ Transformers
- ○ Bus crossties
- ○ AFW pump (PWR)
- ○ Others (specify)

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

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

☐ Diesel-driven pump(s)

☐ Fire protection water pump(s)

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

6. ***Alternative Mitigating Strategy–*** Documentation that supports the use of a unique plant design or operating feature. It is important to note that Section 50.155 of 10 CFR Part 50 requires licensees to have mitigating strategies for beyond-design-basis events, which was created in response to the Fukushima Dai-ichi accident. The strategies, commonly known as FLEX Phase 2 strategies, have been added to the SPAR models. The bases for crediting either a generic or site-specific mitigating strategy or system include:

☐ Engineering analysis or system testing has shown that the mitigating strategy would be successful throughout the accident scenario.

☐ Operating procedures for using the strategy existed at the time of the operational event occurrence.

☐ Operator training for implementing the strategy that existed at the time of the operational event occurrence.

☐ Environmental conditions allow feasible implementation of alternative strategies to cope throughout the accident scenario.

☐ Support systems and instrumentation would be available to support the alternative strategy throughout the accident scenario.

☐ Confirmatory inspections to verify feasibility of alternative strategy.

7. ***Procedures –*** Relevant EOPs, AOPs, severe accident management guidelines and special operating procedures, which were in effect at the time of the event:

☐ Reactor trip and post trip

☐ LOOP event

☐ SBO

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

☐ Recovery of power to the safety buses

☐ Battery life extension (load shedding)

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

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

☐ Switchyard

☐ Safety buses and loads

☐ BOP buses and loads

Note:

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

10.6.1 Initiating Event Analysis of LOOP Event

If a LOOP event (including nonsafety buses) along with a reactor trip occurs, analysts will perform an initiating event analysis (see Section 8 for additional information). Using the ECA workspace, analysts will select the applicable LOOP type (see Section 10.4 for additional information). This selection will activate the proper flag set to ensure the correct non-recovery probabilities are used. If information regarding the details of the LOOP event is well known, including the recovery of offsite power, analysts should use the HRA recovery model to calculate the non-recovery probabilities.

10.6.1.1 HRA Recovery Model

In an analysis of a LOOP initiating event where the event details are well known, including the recovery of offsite power, analysts should use the HRA recovery model to calculate the non-recovery probabilities. Analysts need to review how and when offsite power was recovered during the event. In addition, the licensee may not be in a hurry to restore offsite power during the event because it is expected that the EDGs successfully provided power to the safety buses. If this evaluation determines that offsite power could not be restored within some or all the applicable offsite power recovery times in the SPAR model, the analyst must set the applicable offsite power non-recovery basic events to TRUE. An HRA method (SPAR-H or IDHEAS-ECA) should be used to evaluate the offsite power non-recovery basic events where offsite power recovery was possible.

A task analysis should be performed as part of this evaluation to identify the steps needed to restore power to the first safety bus, given the accident sequence of interest. Complexities of the recovery actions need to be considered, given the context in which each operator action occurs; wherein this context is invariably sequence and cutset specific. Note that the recovery path could be different during postulated SBO conditions than the pathway taken during the event.

The calculated offsite power non-recovery probabilities can be a key source of uncertainty in some initiating event analyses due to the following:

- Timing estimates for postulated scenarios not observed during the event (e.g., SBO).
- Potential grid instabilities after a grid- or weather-related LOOP could result in delays or indecision on restoring offsite power during a postulated SBO.
- PSF/PIF selection.
- Uncertainties associated with the selected HRA method (e.g., cognitive model, timing model, limited data).

10.6.2 Initiating Event Analysis of a Partial LOOP Event

If a partial LOOP event along with a reactor trip occurs, analysts will perform an initiating event analysis (see Section 8 for additional information). The LOOP event trees are not appropriate for modeling partial LOOP events (with a reactor trip). Analysts need to select the most appropriate initiating event to represent what occurred. The event trees for transient initiating events (e.g., general transient, loss of feedwater, loss of condenser heat sink, etc.) are typically the best choice for modeling partial LOOP initiating events. The LOOP to the bus(es) is modeled using the flag events (e.g., HE-LOOP-A, HE-LOOP-B, etc.) or the appropriate electrical component (e.g., transformer, breaker). Note that modeling of the electrical system SSCs upstream of the safety buses in the SPAR model is limited. In addition, not all SPAR models have the correct flag event(s) to model the partial LOOP events. Analysts should consult with the SPAR Model Help Desk if the SPAR model does not have correct logic to support the analysis. Recovery of offsite power to the affected buses needs to be accounted for in the applicable fault tree logic. If credit for offsite power recovery is provided, analysts need to ensure the non-recovery probabilities are appropriate for all applicable sequences/cutsets.

10.6.3 Condition Analysis of a LOOP or Partial LOOP Event

If a LOOP event or partial LOOP event occurs and the plant continues to operate (i.e., no reactor trip occurs), analysts will perform a condition analysis. The LOOP to the bus(es) is modeled using the flag events or the appropriate electrical component. Recovery of offsite power to the affected buses needs to be accounted for in the applicable fault tree logic. If credit for offsite power recovery is provided, analysts need to ensure the non-recovery probabilities are appropriate for all applicable sequences/cutsets.

11 SSIEs

11.1 Objective and Scope

The objective of this guide is to address the use of the fault tree modeling of SSIEs within the SPAR models for SDP, ASP, NOED or MD 8.3 assessments.

11.2 Background

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

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

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

The NRC has decided to incorporate SSIEs for the fluid and air systems in the SPAR models to align with best practices and to meet requirements of the ASME/ANS PRA Standard. PWR SPAR models include loss of service water, loss of CCW, and loss of instrument air initiating event fault trees. BWR SPAR models will include loss of service water, loss of reactor/turbine building closed-loop cooling water, and loss of instrument air initiating event fault trees.[62]

From the three methods proposed for modeling SSIEs in EPRI Technical Report 1016741, the NRC has selected the explicit event methodology (i.e., carry the fault tree logic cutsets through the event tree) in the SPAR models.[63] This decision was made in part because of the method's ability to illustrate the basic event contribution to the initiating event total frequency and allow the same components to be failed when analyzing the other event trees (e.g., transient). In addition, the impact of the individual components can be viewed in the cutsets and importance measures.

11.3 Explicit Event Methodology

The explicit event methodology uses both initiating events and enabling events to represent each component or train within a support system. Both representations are needed for each component or train since a failure of a support system usually requires multiple components to

[62] SSIEs that contribute less than 1 percent of the total plant CDF have been excluded from SPAR models.

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

fail simultaneously or within a brief period. Therefore, the initiating event causes the loss of the support system if and only if the appropriate enabling events (i.e., additional component failures) are present. Initiating events are quantified as the frequency at which each component or train fails in a year. The enabling events represent the component's unavailability, or the probability the component will fail or be in a failed state at the time of an initiating event.

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

11.4 SPAR Model Manipulations for ECA

To perform an initiating event analysis for a total loss of a support system, analysts should perform the following steps:

- Select the applicable initiating event (e.g., loss of service water, CCW, instrument air, etc.) and set its probability to 1.0. The probabilities of all other initiating events should be set to zero.
- Set the applicable SSIE fault tree initiating event(s) (e.g., failure of a running service water pump, CCW pump, instrument air compressor, or operating heat exchanger, etc.) to TRUE. In addition, any applicable enabling events (e.g., failure of standby service water pump, CCW pump, instrument air compressor, heat exchanger, etc.) should be set to TRUE, if needed.
- Set the corresponding basic event(s) for the failed component(s) that are included within the applicable support system fault tree(s) to TRUE.

  Example – With CCW pumps 'A' and 'C' running and CCW pump 'B' in standby, a CCF of both running pumps occurs. In addition, the standby pump fails to start resulting in a complete loss of CCW. Analysts would set the probability of the loss of CCW initiating event to 1.0 and the probabilities of the other initiating events to 0. In addition, analysts would set the initiating event for CCF FTR of pumps 'A' and 'C' and the enabling event for FTS of pump 'B' to TRUE. Analysts would also set the corresponding basic event for CCF FTR of pumps 'A' and 'C' to TRUE.[64] Note that the enabling event for the FTS of pump 'B' is the same basic event used in the applicable support system fault tree(s) and, therefore, no additional modifications are needed.

To perform a condition analysis of a support system component(s) failure, analysts should perform the following steps:

- For a failure of a running/operating support system component:
  - Set the applicable initiating event to FALSE for the failed component.[65]

[64] Some SPAR models may not have CCF basic events for the different component combinations (i.e., there is a single CCF event that includes all possible CCF combinations for the applicable failure mode. In these cases, analysts should contact the SPAR Model Help Desk for assistance on making the appropriate model changes.

[65] The corresponding initiating event basic event is set to FALSE because a loss of CCW initiating event did not occur. Note that this modeling assumption will potentially underestimate the increase to the initiating event frequency.

    - ○ Set the corresponding basic event for the failed component that is included within the applicable support system fault tree(s) to TRUE.
    - ○ If the support system components were in a specific configuration for the entire exposure period, set the appropriate configuration basic events accordingly.

      Example – For the past 15 days, CCW pumps ‘A’ and ‘C’ were running, with CCW pump ‘B’ in standby. Pump ‘A’ fails while running and pump ‘B’ successfully auto-starts and runs. It takes the licensee 2 days to repair the pump and, therefore, the exposure period is approximately 2 days. Analysts would set the initiating event for FTR of pump ‘A' to FALSE and the corresponding basic event for FTR of pump ‘A included within the applicable support system fault tree(s) to TRUE. Since the exposure time essentially starts with pump ‘A’ unavailable, and pumps ‘B’ and ‘C’ running, analysts would set the configuration event for CCW pumps ‘B’ and ‘C’ running, pump ‘A’ in standby to TRUE, and set the other configuration events to FALSE.

- – For a failure of a standby support system component:
    - ○ Set the applicable enabling basic event for the failed component that is included within the applicable SSIE fault tree to TRUE. Note that the enabling event is the same basic event used in the applicable support system fault tree(s) and, therefore, no additional modifications are needed.
    - ○ If there is no enabling basic event, set the corresponding basic event for the failed component that is included within the applicable support system fault tree(s) to TRUE.
    - ○ If the support system components were in a specific configuration for the entire exposure period, set the appropriate configuration basic events accordingly.

      Example – For the past 15 days, CCW pumps ‘A’ and ‘C’ were running, with CCW pump ‘B’ in standby. While attempting to shift to pump ‘B’ operating in place of pump ‘A’, pump ‘B’ fails to start. Pump ‘B’ last run successfully 15 days ago and inspectors determined that the pump would not have successively started given a postulated demand during this entire period. It takes the licensee 2 days to repair the pump, and, therefore, the exposure period is approximately 17 days. Analysts would set the enabling event for FTS of pump ‘B’ to TRUE. Note that the enabling event for the FTS of pump ‘B’ is the same basic event used in the applicable support system fault tree(s) and, therefore, no additional modifications are needed. Since the pumps ‘A’ and ‘C’ were running during the entire 17-day exposure time, analysts would set the configuration event for CCW pumps ‘A’ and ‘C’ running, pump ‘B’ in standby to TRUE, and set the other configuration events to FALSE.

11.5 Remaining Technical Issues

Some CCF modeling techniques (see Section 5.5) have not been fully developed, reviewed, and/or accepted by the staff/PRA community. These issues include (not an exhaustive list): the potential underestimation of the increases to initiating event frequencies given a failure operating components, using the SAPHIRE CCF methodology for SSIE models, the conditional treatment of CCFs in the SSIE fault tree, and any additional issues identified during the initial use of the SSIE models. The accuracy of the cutset-based results can vary depending on the SSIE model repair assumptions. In addition, the cutsets may not capture the significant transient behavior of SSIE frequencies for time periods that may be encountered in an ECA. The importance measures associated with the SSIE models calculated within the ECA workspace in SAPHIRE can be in error due to the explicit method calculation and depending on the analysis assumptions.

References Section 12

12 References

1. U.S. Nuclear Regulatory Commission, "NRC Incident Investigation Program," Management Directive 8.3, May 2023 (ML22294A067).

2. U.S. Nuclear Regulatory Commission, "Significance Determination Process," Inspection Manual Chapter 0609, January 2025 (ML24257A157).

3. U.S. Nuclear Regulatory Commission, "Reactor Oversight Process Basis Document," Inspection Manual Chapter 0308, January 2025 (ML24269A231).

4. U.S. Nuclear Regulatory Commission, "Reactive Inspection Decision Basis for Power Reactors," Inspection Manual Chapter 0309, December 2023 (ML23234A176).

5. U.S. Nuclear Regulatory Commission, "Risk Assessment of Operation Events Handbook – External Events," Volume 2, Revision 1.01, January 2008 (ML080300179).

6. U.S. Nuclear Regulatory Commission, "Risk Assessment of Operation Events Handbook – SPAR Model Reviews," Volume 3, Revision 2, September 2010 (ML102850267).

7. U.S. Nuclear Regulatory Commission, "Risk Assessment of Operation Events Handbook – Shutdown Events," Volume 4, Revision 1, April 2011 (ML111370163).

8. U.S. Nuclear Regulatory Commission, "PRA Review Manual," NUREG/CR-3485, September 1985 (ML20135H483).

9. American Society of Mechanical Engineers, "Addenda to ASME/ANS RA-S-2008 Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications," RA-Sa-2009, February 2009.

10. U.S. Nuclear Regulatory Commission, Regulatory Guide 1.200, "An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities," Revision 3, December 2020 (ML20238B871).

11. U.S. Nuclear Regulatory Commission, "Handbook of Parameter Estimation for Probabilistic Risk Assessment," NUREG/CR-6823, September 2003 (ML032900131).

12. U.S. Nuclear Regulatory Commission, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," NUREG/CR-6928, February 2007 (ML070650650).

13. U.S. Nuclear Regulatory Commission, "Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment," NUREG/CR-5485, November 1998 (ML20198E585).

14. Idaho National Laboratory, "CCF Parameter Estimations, 2020 Update," INL/EXT-21-62940, Revision 1, August 2022.

15. U.S. Nuclear Regulatory Commission, “CCCG Modeling and Treatment of Cross-Unit CCFs,” April 2025 (ML25105A198).

16. Idaho National Laboratory, “Developing Component-Specific Prior Distributions for Common Cause Failure Alpha Factors,” INL/EXT-21-65527, Revision 2, May 2024.

17. U.S. Nuclear Regulatory Commission, “Technical Basis for Significance Determination Process,” Inspection Manual Chapter 0308, Attachment 3, January 2025 (ML24257A172).

18. U.S. Nuclear Regulatory Commission, “CCF Work Summary and Conclusions,” March 2021 (ML21055A027).

19. U.S. Nuclear Regulatory Commission, “Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding,” NURE/CR-6268, September 2007 (ML072970404).

20. Idaho National Laboratory, “Causal CCF Parameter Estimations 2020,” INL/RPT-23-72728, May 2023.

21. U.S. Nuclear Regulatory Commission, “Good Practices for Implementing Human Reliability Analysis (HRA),” NUREG-1792, April 2005 (ML051160213).

22. U.S. Nuclear Regulatory Commission, “NRC Staff Position on Crediting Mitigating Strategies Implemented in Response to Security Orders in Risk-Informed Licensing Actions and in the Significance Determination Process,” Regulatory Information Summary 2008-15, June 2008 (ML080630025).

23. Nuclear Energy Institute, “Qualitative Assessment for Crediting Portable Equipment in Risk-Informed Decision Making,” December 2015 (ML16138A018).

24. Nuclear Energy Institute, “Streamlined Approach for Crediting Portable Equipment in Risk-Informed Decision Making,” December 2015 (ML16138A017).

25. U.S. Nuclear Regulatory Commission, Memorandum from W. Dean (NRC) to A. Pietrangelo (NEI), August 9, 2016 (ML16167A034).

26. Nuclear Energy Institute, “Crediting Mitigating Strategies in Risk-Informed Decision Making” NEI-16-06, August 2016 (ML16286A297).

27. U.S. Nuclear Regulatory Commission, “Assessment of the Nuclear Energy Institute 16-06, ‘Crediting Mitigating Strategies In Risk-Informed Decision Making,’ Guidance For Risk-Informed Changes To Plants Licensing Basis,” Memorandum form M. Reisi-Fard to J. Giitter, May 30, 2017 (ML17031A269).

28. U.S. Nuclear Regulatory Commission, “Updated Assessment of Industry Guidance for Crediting Mitigating Strategies in Probabilistic Risk Assessments,” Memorandum form A. Zoulis to M. Franovich, May 6, 2022 (ML22014A084).

29. U.S. Nuclear Regulatory Commission, “SPAR-H Human Reliability Analysis Method,” NUREG/CR-6883, August 2005 (ML15142A653).

30. U.S. Nuclear Regulatory Commission, “Integrated Human Event Analysis System for Event and Condition Assessment (IDHEAS-ECA),” NUREG-2256, October 2022 (ML22300A117).

31. U.S. Nuclear Regulatory Commission, “A Review of NRC Staff Uses of PRA,” NUREG-1489, June 2007, (ML063540593).

32. Idaho National Laboratory, “SPAR-H Step-by-Step Guidance,” INL/EXT-10-18533, Revision 2, May 2011 (ML112060305).

33. U.S. Nuclear Regulatory Commission, “The General Methodology of an Integrated Human Event Analysis System (IDHEAS-G),” NUREG-2198, May 2021 (ML21127A272).

34. U.S. Nuclear Regulatory Commission, “IDHEAS-ECA Evaluations of SPAR Model Human Failure Events,” RIL 2024-17, January 2025 (ML24352A019).

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

36. U.S. Nuclear Regulatory Commission “Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications,” NUREG-1278, August 1983 (ML071210299).

37. U.S. Nuclear Regulatory Commission, “Integrated Human Event Analysis System Dependency Analysis Guidance (IDHEAS-DEP),” Research Information Letter 2021-14, November 2021 (ML21316A107).

38. U.S. Nuclear Regulatory Commission, “Reevaluation of Station Blackout Risk at Nuclear Power Plants,” NUREG/CR-6890, Volume 1, December 2005, (ML060200477).

39. Idaho National Laboratory, “Analysis of Loss-of-Offsite-Power Events 2023 Update,” INL/RPT-24-79969, July 2024.

40. Idaho National Laboratory, “Analysis of Loss of Offsite Power Events 2020 Update,” INL/EXT-21-64151, November 2021.

41. Pressurized Water Reactor Owner’s Group, “FLEX Equipment Data Collection and Analysis,” PWROG-18042-NP, February 2022 (ML22123A259).

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